AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBER THREATS TO CAPITAL MARKETS AND CORPORATE ACCOUNTS

HEARING

BEFORE THE

SUBCOMMITTEE ON CAPITAL MARKETS AND
GOVERNMENT SPONSORED ENTERPRISES

OF THE

COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JUNE 1, 2012

Printed for the use of the Committee on Financial Services

Serial No. 112–131

U.S. GOVERNMENT PRINTING OFFICE
76–102 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

SPENCER BACHUS, Alabama, *Chairman*

JEB HENSARLING, Texas, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
RON PAUL, Texas
DONALD A. MANZULLO, Illinois
WALTER B. JONES, North Carolina
JUDY BIGGERT, Illinois
GARY G. MILLER, California
SHELLEY MOORE CAPITO, West Virginia
SCOTT GARRETT, New Jersey
RANDY NEUGEBAUER, Texas
PATRICK T. McHENRY, North Carolina
JOHN CAMPBELL, California
MICHELE BACHMANN, Minnesota
THADDEUS G. McCOTTER, Michigan
KEVIN McCARTHY, California
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
NAN A. S. HAYWORTH, New York
JAMES B. RENACCI, Ohio
ROBERT HURT, Virginia
ROBERT J. DOLD, Illinois
DAVID SCHWEIKERT, Arizona
MICHAEL G. GRIMM, New York
FRANCISCO “QUICO” CANSECO, Texas
STEVE STIVERS, Ohio
STEPHEN LEE FINCHER, Tennessee

BARNEY FRANK, Massachusetts, *Ranking Member*
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELÁZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
RUBÉN HINOJOSA, Texas
WM. LACY CLAY, Missouri
CAROLYN McCARTHY, New York
JOE BACA, California
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JOE DONNELLY, Indiana
ANDRÉ CARSON, Indiana
JAMES A. HIMES, Connecticut
GARY C. PETERS, Michigan
JOHN C. CARNEY, JR., Delaware

JAMES H. CLINGER, *Staff Director and Chief Counsel*

SUBCOMMITTEE ON CAPITAL MARKETS AND GOVERNMENT SPONSORED ENTERPRISES

SCOTT GARRETT, New Jersey, *Chairman*

DAVID SCHWEIKERT, Arizona, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
DONALD A. MANZULLO, Illinois
JUDY BIGGERT, Illinois
JEB HENSARLING, Texas
RANDY NEUGEBAUER, Texas
JOHN CAMPBELL, California
THADDEUS G. McCOTTER, Michigan
KEVIN McCARTHY, California
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
NAN A. S. HAYWORTH, New York
ROBERT HURT, Virginia
MICHAEL G. GRIMM, New York
STEVE STIVERS, Ohio
ROBERT J. DOLD, Illinois

MAXINE WATERS, California, *Ranking Member*
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
RUBÉN HINOJOSA, Texas
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
CAROLYN B. MALONEY, New York
GWEN MOORE, Wisconsin
ED PERLMUTTER, Colorado
JOE DONNELLY, Indiana
ANDRÉ CARSON, Indiana
JAMES A. HIMES, Connecticut
GARY C. PETERS, Michigan
AL GREEN, Texas
KEITH ELLISON, Minnesota

CONTENTS

Page

Hearing held on:
  June 1, 2012 1
Appendix:
  June 1, 2012 39

WITNESSES

FRIDAY, JUNE 1, 2012

Cantley, Michele B., Chief Information Security Officer, Regions Bank, on behalf of the Financial Services Information Sharing and Analysis Center ... 4
Clancy, Mark G., Managing Director and Corporate Information Security Officer, The Depository Trust & Clearing Corporation (DTCC) 6
Graff, Mark, Vice President and Chief Information Security Officer, NASDAQ OMX 7
Smocer, Paul, President, BITS, Technology Policy Division of the Financial Services Roundtable 9
Weiss, Errol, Director, Cyber Intelligence Center, Citi, on behalf of the Securities Industry and Financial Markets Association (SIFMA) 11
Woodhill, James R., Advocate, Government and Public Relations, YourMoneyIsNotSafeInTheBank.org 12

APPENDIX

Prepared statements:
  Hurt, Hon. Robert 40
  Cantley, Michele B. 41
  Clancy, Mark G. 64
  Graff, Mark 78
  Smocer, Paul 82
  Weiss, Errol 90
  Woodhill, James 100

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Schweikert, Hon. David:
  Written responses to questions submitted to Errol Weiss 120

CYBER THREATS TO CAPITAL MARKETS AND CORPORATE ACCOUNTS

Friday, June 1, 2012

U.S. House of Representatives,
Subcommittee on Capital Markets and
Government Sponsored Enterprises,
Committee on Financial Services,
Washington, D.C.

The subcommittee met, pursuant to notice, at 9:35 a.m., in room 2128, Rayburn House Office Building, Hon. Scott Garrett [chairman of the subcommittee] presiding.

Members present: Representatives Garrett, Schweikert, Manzullo, Biggert, Neugebauer, Posey, Hurt, Grimm, Stivers, Dold; Lynch, and Maloney.

Chairman GARRETT. Today's hearing of the Subcommittee on Capital Markets and Government Sponsored Enterprises is called to order. Today's hearing is entitled, "Cyber Threats to Capital Markets and Corporate Accounts." I appreciate the entire panel being with us today, and I look forward to an interesting, albeit at times, a somewhat technical hearing. So I look forward to the entire testimony of the witnesses and the questions that will follow. At this time, we will move to opening statements.

I yield myself 4 minutes.

Again, what we are talking about today is cyber attacks and the threat of cyber attacks against our economic interests. As we learned from this panel, as well as from people who have visited our offices, and the media, this issue is a growing concern to many here on the committee. And so, a better understanding of the potential dangers that cyber criminals, if you will, pose to consumers, financial institutions, and government agencies will help improve our chances to avoid disruption in the financial markets. There have been a number of high-profile cyber attacks over the past several years. Known intrusions into public Web sites have occurred at the Department of Defense; the International Monetary Fund; and Booz Allen Hamilton.

In December 2011, the U.S. Chamber of Commerce reported that its computer networks had been compromised and that confidential communications and industry positions were accessed. A lot of financial services providers are big targets, of course—according to legend, Willie Sutton said that he robbed banks "because that's where the money is." Financial services businesses have been leaders in an effort to armor their data networks and to identify and deal with any actual breaches as quickly and as transparently as possible.

The costs to business consumers are difficult to quantify, but we must ensure that we have the proper safeguards in place to thwart or minimize future attacks while simultaneously protecting the privacy of all the citizens. Consumer confidence, therefore, plays a significant role in any financial transaction or investment either by an individual or by a small business. Unfortunately, just as there have been numerous instances of identity theft out there where individuals have credit cards stolen or accounts looted, there has also been a significant rise in corporate account takeovers as well.

Cyber threats come in many different shapes and sizes. We are all familiar with the threat of identity theft; I know about that. According to a recent Javelin strategy and research study, identity theft cost Americans $37 billion in 2010 alone. So today, I can't think of a less appetizing scenario than having someone other than myself accessing my personal banking information for their personal benefit.

Additionally, there has been a significant increase in corporate account takeovers, which are essentially identity theft of a company instead of a business or an individual. Consequently, small businesses are seeking solutions to safeguard their information and their finances.

Our financial markets and clearinghouses have largely been spared the high-profile attacks that have succeeded at some banks partially because of their hard work and partially because of the way they are constructed. But they are still vulnerable to denial of service attacks on public Web sites or on utilities that serve them.

Fortunately, as we saw in the terrible attacks a decade ago in New York City, our markets are resilient, and I am confident they have only become more resilient and more reliable ever since. But it is important to let them tell their story today in their own words. And so, we are holding these hearings to discuss current and potential threats against our financial services industry and to discuss how we together can be better prepared against future attacks.

We must remember that we always remain vigilant when we are protecting personal and financial information. So much of our economy is reliant on the Internet today that we must not be complacent in all of this. Our economy has always been a leading contributor to our national strength. We must ensure that it is protected against tomorrow's threats. So I thank you again for coming, and for your testimony which will follow, and at this point, I yield back and yield to the gentlelady from New York for 3 minutes.

Mrs. MALONEY. Thank you. I will be very, very brief. Certainly the security of our financial markets, our government, is incredibly important to our national and personal security, and today's hearing is part of a continuing oversight and dialogue we are having in Congress about the threats to our markets and the impact these attacks could have on our economy, on our individuals, and on our government. And with the rapid pace of technology and the growing number of threats across a wide range of businesses, both large and small, it is truly a huge, huge challenge and one that needs absolute total commitment and coordination between the public and the private sector to protect our markets, to protect individuals, and to protect our government.

I do want to mention a recent report by Symantec, the "Internet Security Threat Report," which was excellent. It stated that half of our businesses in America, both big and small, were targeted by cyber attacks, and over 232 million identities were stolen in 2011, including my own. There is a "Carolyn Maloney" running around Maryland. This is truly a wake-up call.

In their report, they say that 5.5 billion total attacks were blocked in 2011. So not only do we have to look at ways to continue to block this, but we need to continue to look at ways to protect our capital markets and our industries, both public and private, the information that we have.

I look forward to hearing from the witnesses today, and I yield back. Thank you.

Chairman GARRETT. Thank you. The gentlelady yields back. The gentleman from Arizona for 2 minutes.

Mr. SCHWEIKERT. Thank you, Mr. Chairman. I will try to be fairly quick. What I am hoping to actually hear from the panel—actually, Mrs. Maloney, should I be worried that there is another one of you running around Maryland?

Mrs. MALONEY. There is. The FBI is looking for her.

Mr. SCHWEIKERT. It is a combination of things. First off, right now, with the way we allocate liability, are we creating incentives or disincentives for some folks within, shall we say, the financial food chain to invest and others to not invest? This is sort of a side concern.

Second of all, I would like to hear and understand how, throughout the industry, you coordinate talent, coordinate technology, and coordinate data and information of best practices. Third, I want you to either assuage me or agree with me; I am one of the Members of Congress who actually has a great concern that a growing governmental role in the whole issue of cyber attacks and data protection—that government so often becomes bureaucratic and moves so slowly that it will actually make reaction time worse, and therefore raise our exposure. That is a concern, and I would like some definition back of, in many ways, are we making it more difficult to react on an instant time? So with that, Mr. Chairman, I yield back.

Chairman GARRETT. Thank you. Mr. Dold is recognized now for 2 minutes.

Mr. DOLD. Thank you. Mr. Chairman, I certainly appreciate you holding this hearing on a very important topic and I want to thank our witnesses for taking your time and joining us today. I believe our capital markets are a critical driver of our economy and our Nation's productivity, and our technology is the most advanced in the world. But today we are facing a constantly increasing threat of cyber crime and cyber intrusions. Sophisticated viruses and malware threaten our commercial businesses and individuals, costing us billions of dollars each and every year while also threatening our power grids and our national security.

That is why it is so critical to focus on this issue and to strengthen the safety and integrity of our financial sector against cyber threats.

Every day, literally hundreds of thousands of cyber threats hit our financial institutions. I think that is something that not many people really recognize, and it is something that we need to be prepared to act against.

In that regard, I am confident that my colleagues and I share several bipartisan goals. First, we must maintain and improve our existing cybersecurity infrastructure and identify all cybersecurity breaches.

Second, we must share all relevant cyber threat information to facilitate a fast and effective response. And we must do this in a way that does not unduly infringe upon privacy rights, consumer rights or the integrity of business contracts.

Third, the private sector and the public sector must work together in leveraging existing institutions to evolve with the increasing cyber attack complexity.

Finally, the private sector must be able to work confidently with law enforcement agencies to protect the existing systems while ensuring that sensitive information is handled securely and is used appropriately.

Clearly, to maintain the public trust, the financial sector and government agencies must remain committed to protecting personal data and intellectual property. I want to thank you again for being here, and Mr. Chairman, I want to thank our witnesses for sharing their time, their testimony, and their experience with us today. That you so much. I yield back.

Chairman GARRETT. The gentleman yields back, and I echo those remaining comments of the gentleman to the panel as well, and seeing no other opening statements, I will now turn to our panel for your opening statements.

As always, for those of you who have not been here before, you will be recognized for 5 minutes. Your complete written testimony will be made a part of the record, and you can summarize what you have in front of you.

So, we will turn first to Ms. Cantley. Good morning. You are recognized for 5 minutes.

STATEMENT OF MICHELE B. CANTLEY, CHIEF INFORMATION SECURITY OFFICER, REGIONS BANK, ON BEHALF OF THE FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER

Ms. CANTLEY. Good morning. Chairman Garrett, Representative Maloney, and members of the subcommittee, my name is Michele Cantley. I am the chief information security officer for Regions Bank, and I am appearing today for the Financial Services Information Sharing & Analysis Center, FS-ISAC. I want to thank you for this opportunity to address the subcommittee on the important issue of corporate account takeover.

I have been head of information security at Regions since 2004. Regions is the 12th largest bank by deposits and loans and it serves customers in 16 States. Regions is a member of the FS-ISAC, an organization formed in 1999 by a Presidential order with the mission of protecting the financial services sector against cyber and physical threats and risk.

Today, the FS-ISAC has more than 4,400 member organizations that represent the majority of the U.S. financial services industry.

It is important to note that industry has spent much time and effort and has worked closely with its regulators and other interested parties to provide safe systems to its customers. The FS-ISAC is aware, through its information-sharing arrangements with both public and private sector organizations, that criminal actors are targeting our sector. Corporate account takeover is one method of attack. Corporate account takeover is the unauthorized use of online banking credentials typically obtained via malicious software, malware, that affects customers' computers, work stations, or networks. Cyber criminals continue to attack business customers' computers by phishing, which remains the most popular form of attack through malicious advertisements and by fraudulent messages on social media sites. In each case, the cyber criminals attempt to trick their victims into clicking on a bogus link that redirects the unknowing user to a server that then downloads malware onto the victim's computer.

This software includes a program that captures the user's online banking credentials as he types them and allows the criminal to impersonate the customer and create fraudulent financial transactions.

Over the past 2 years, losses experienced by financial institutions and their customers as a result of cyber-related fraud have declined even as the number of attacks has increased. The FS-ISAC and its members recognize the threat both to the affected institutions and to customer confidence posed by these criminal acts.

In 2010, as part of our active efforts to counteract the threat of corporate account takeover, the FS-ISAC formed the account takeover task force. The task force consists of over 120 individuals from financial firms and government agencies. Its recently completed report recommends three main areas of focus—prevention, detection, and response—in order to ensure and improve an effective defense against account takeover.

The FS-ISAC and its membership have taken tremendous steps to limit cyber crime and corporate account takeover. Nonetheless, corporate account takeover attempts cannot be stopped solely by the financial institutions. All participants in the Internet ecosystem have roles to play. Banks, for instance, have no direct control over the end customer's computers nor can banks control what e-mails bank customers open or what Web sites they visit prior to accessing their online banking systems.

Still, to increase the security of our customers' accounts, we must educate our customers on the risks, monitor for anomalous transactions, and stop fraudulent transactions we detect.

Customers have a role to play in learning about these threats and practicing safe Internet habits. Internet service providers and e-mail providers can monitor traffic on their networks for much of this malware and alert their customers to these threats.

Finally, the FS-ISAC believes that the private sector and government can continue to work together to improve Internet security. One area I would highlight is that law enforcement should continue to move aggressively against cyber criminals and that more work on international, legal, and diplomatic levels is needed so that all countries recognize this type of cyber crime.

I look forward to any questions that you might have and thank you for the opportunity to appear before your subcommittee today.

[The prepared statement of Ms. Cantley can be found on page 41 of the appendix.]

Chairman GARRETT. And we thank you as well.

Mr. Clancy, you are recognized for 5 minutes, and welcome.

STATEMENT OF MARK G. CLANCY, MANAGING DIRECTOR AND CORPORATE INFORMATION SECURITY OFFICER, THE DEPOSITORY TRUST & CLEARING CORPORATION (DTCC)

Mr. CLANCY. Good morning, Chairman Garrett and Ranking Member Waters. My name is Mark Clancy, and I am the corporate information security officer at the Depository Trust & Clearing Corporation. DTCC is a participant-owned and governed cooperative that serves as critical infrastructure for the U.S. capital markets and financial markets globally.

Our operations and processes are essential to mitigating risk and ensuring the safe and efficient operation of the financial system. Cyber crime poses a significant threat to capital markets globally. A study by the U.S. Treasury found that cyber crime accounts for more revenue than international drug cartel income, running into the hundreds of billions of dollars annually.

There are three main types of cyber attacks aimed at the financial sector. The first involves the theft of confidential data. In its most insidious form, cyber criminals take over the accounts of innocent victims globally and either directly steal funds or use the stolen credentials for market manipulation by what is called "pump and dump" scams. Their goal is to move the market in a stock by bidding against themselves and anyone else they can lure into the scam.

In recent years, DTCC has also witnessed data theft in our industry involving highly sophisticated social engineering techniques that attempt to give foreign entities a competitive advantage in negotiations often related to winning bids for natural resources or beating the offering price for an acquisition of a company.

The second type of attack involves compromising the integrity of the National Market System, NMS, in the United States. The goal of these cyber crimes is to grind the financial system to a halt and disrupt national economies. While there are no public reports of the NMS directly being impacted today, an attack on the Hong Kong Stock Exchange in 2011 reinforced the dangers of this threat.

The third type of attack involves compromising the integrity of financial data, which today exists overwhelmingly in digital form. These attacks have the potential to be the most catastrophic. For example, the European market for carbon credit trading was the victim of such an attack in January 2011 when cyber criminals changed the ownership information of individual carbon credits. This resulted in the theft of 30 million euros' worth of credits from the European emissions market and the closure of the EU Emissions Trading System for more than a week.

While financial institutions have robust information security programs in place to protect their systems from cyber threats, these programs are not foolproof. A critical resource the industry relies upon to safeguard the system is information sharing between Federal agencies and financial institutions, most notably via the Financial Services Information Sharing and Analysis Center.

I would like to focus on a successful but now defunct pilot program known as the Government Information Sharing Framework, GISF, which targeted cyber espionage. Under the program, 16 financial services firms were granted access to advanced threat and attack data as well as classified technical and analytical data on threat identification and mitigation techniques. The GISF program provided the sector with access to actionable information to search for similar threat activity in their own networks, access to contextual information to better understand risk implications to various threats, the ability to adjust assessments of cyber espionage using quantifiable information that had previously been unavailable, and a better understanding of the need to develop standards to support the automation of sharing and consuming threat data.

The GISF program drove innovation and new initiatives in the industry and helped reshape the sector's approach to assessing cyber espionage risks. It also prompted pilot firms, including DTCC, to revise best practices.

Unfortunately, the program was effectively terminated in December 2011 for reasons that were unclear. Since then, more than five financial institutions have experienced threat activity from actors first identified through GISF reporting.

Furthermore, an assessment by the FS-ISAC found that these threats will continue to increase in the future. Information sharing like that which occurred under GISF represents the most critical line of defense in managing and mitigating cyber risk today.

DTCC strongly supports restarting GISF's program, removing its pilot status, and expanding its reach within the financial sector.

As the sophistication and technological means of cyber criminals increases, the financial sector in government needs to move from a static "one-size-fits-all" framework to a risk-based one that incorporates the dynamic nature of cybersecurity threat landscape.

While the public and private sectors have taken important steps in recent years to enhance collaboration, a greater degree of information sharing and trust is needed to ensure that all resources are working in concert to protect and defend the financial sector from cyber attack.

DTCC stands ready to work in partnership with this committee, the Congress, and the Administration to harden the sector's defenses against cyber crimes.

Thank you for your time.

[The prepared statement of Mr. Clancy can be found on page 64 of the appendix.]

Chairman GARRETT. I thank you, as well.

Mr. Graff is recognized for 5 minutes. Welcome.

STATEMENT OF MARK GRAFF, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, NASDAQ OMX

Mr. GRAFF. Thank you, Chairman Garrett, Ranking Member Waters, and members of the subcommittee. My name is Mark Graff, and I am the vice president and chief information security officer (CISO) for NASDAQ OMX. Although I am new to NASDAQ OMX, having arrived just this past April, I am no newcomer to information security with about 25 years' experience serving both the industry and government. Most recently, I was head of cybersecurity at Lawrence Livermore National Laboratory which is not only one of the crown jewels of research in this country, but also the repository of some of the Nation's most important secrets, including nuclear weapons designs.

I moved to NASDAQ OMX to help protect another part of America's critical infrastructure—its financial markets. I changed industries, but most of the challenges remain just the same.

NASDAQ OMX is committed to a vigorous defense of its critical infrastructure, and as an expert in the methods used today to defend this Nation's most critical, most highly classified systems from attack, I can tell you that many of these same techniques and technologies are used to defend NASDAQ OMX.

One key method at both institutions is the isolation of critical systems from the Internet at large. While many of the servicers who deliver to customers worldwide are housed on Internet facing Web servers, our trading and market systems are safely tucked away behind several layers of carefully arranged barriers, such as firewalls and network isolation zones. This is an important distinction to remember, and we should all keep this in mind when we hear about denial of service attacks against one institution or another. Any troublemaker can run up to the front door of a house and ring the doorbell over and over again—and that is what most denial of service attacks amount to—if sometimes despite our best efforts, our customers are unable to reach one of our outward facing Web sites for a few minutes as a result of this kind of vandalism, I ask us all to remember that it doesn't mean, in my homely analogy, that someone has broken into the house. Market systems remain secure.

But we don't rely on isolation alone. We have a comprehensive information security program using a multi-layered approach. For example, in developing software we treat information security as a critical element all the way through the life cycle of the software from design to implementation, and also in everyday use.

These controls that I have talked about span our entire enterprise network. Our trading systems, though, are further protected by their overall resilient architecture. While these trading platforms, as I mentioned, are isolated from the rest of the network and from the Internet, the system also restricts the information that is allowed to be submitted to it through the use of a fixed set of formatted protocols that control inputs to the trading platform.

It also is refreshed at the end of the trading day, every information trading system and no data is maintained in the trading platform beyond the trading day. This helps secure the trading markets which are so important to us.

Now for all those steps, we do have serious concerns about the worldwide attacks on critical infrastructure that are being led not just by rogue hackers and organized crime but by national governments today. And it is our position that it is not reasonable to expect individual companies, no matter how large or sophisticated, to independently stave off cyber attacks that are coordinated and backed by a foreign government.

So it is for this reason that we at NASDAQ OMX are very pleased that both Houses of Congress are looking at ways to protect our critical national infrastructure through improved sharing of information about cyber threats and vulnerabilities. We support the House passage of H.R. 3523, the Cyber Intelligence Sharing and Protection Act. Although there are some concerns about data privacy that certainly may be addressed, we think it is an excellent move forward in this area.

NASDAQ OMX is and continues to be a willing partner with industry peers and government at every level, cooperating to protect the integrity of our critical infrastructure. And it would be my pleasure as NASDAQ OMX's new CISO to continue and expand such contacts and relationships.

Thank you again for inviting me to testify.

[The prepared statement of Mr. Graff can be found on page 78 of the appendix.]

Chairman GARRETT. And thank you.

Mr. Smocer is recognized for 5 minutes. Welcome to the panel.

STATEMENT OF PAUL SMOCER, PRESIDENT, BITS, TECHNOLOGY POLICY DIVISION OF THE FINANCIAL SERVICES ROUNDTABLE

Mr. SMOCER. Thank you, Chairman Garrett, Representative Maloney, and members of the subcommittee. My name is Paul Smocer and I am the president of BITS, which is the technology policy division of the Financial Services Roundtable.

As the recent passage of key legislation during cyber week indicates, the House clearly understands the importance of cybersecurity. Likewise, the financial services industry recognizes the serious and constantly evolving nature of cyber threats to its customers, its institutions, and the broader U.S. economy.

Individual institutions conduct ongoing risk assessments to identify potential institutional and customer threats and to limit these risks for both their own operations and those of their key service providers. This includes providers of services such as clearings, settlements, and accounting within the capital markets environment.

These assessments help assure that the institutions and financial infrastructure such as capital markets remain secure. In the battle over cybersecurity, however, no one institution can fight alone. Consequently, at the sector level, several collaborative efforts exist. The associations such as BITS and other institutions ban together to collectively identify cyber risk, and more importantly, to develop best practices to improve cybersecurity, reduce fraud, and improve resiliency. The largest of these industry collaborations is perhaps the sector's Financial Services Sector Coordinating Council, consisting of the major financial trade associations, the largest U.S.-based financial institutions, and key financial infrastructure participants.

The Council works closely with its public sector partner, the Financial and Banking Information Infrastructure Committee. Chaired by the Treasury Department, this Committee includes 16 government agencies with regulatory oversight for the financial sector including capital markets. Working together, Council and Committee members focus on key cybersecurity issues, including the ability to recover vital infrastructures impacted by cyber or physical incidents.

The two groups sponsor industrywide resiliency exercises, the latest of which had a focus on the resiliency of the equities clearing and trading processes. BITS and other associations have also formed collaborative relationships with various law enforcement agencies to coordinate efforts in preventing and prosecuting cyber crime. The industry also conducts outreach efforts to other key sectors. One recent example is participation in the industry BOTNET group. This multi-industry, multi-stakeholder group is acting collaboratively to mitigate the problem of device takeovers by cyber criminals.

These types of efforts are consistent with the financial services industry's recognition that today's cyber world is highly integrated and relies on multiple organizations and providers to effectively mitigate security risks. The industry also recognizes the importance of cybersecurity education. Consumers and businesses play a key role in cybersecurity and have a responsibility to protect themselves, though the industry and others have recognized that they often lack the skills and awareness to fully do so. As a result, institutions and associations have made significant educational investments.

A key collaborative area of particular note is threat information sharing. Financial institutions currently share threat information via the FS-ISAC. Broader inter-industry and public-private information-sharing opportunities do remain. Because of the interdependency of sectors in key infrastructures such as capital markets, it is vital to share information across a broad swath of sectors to improve the responsiveness and the defense of all sectors.

Maintaining the confidentiality of shared information, particularly between the private and public sectors, however, remains a concern. Organizations are concerned that revelation of information will impact their reputation and their customers' confidence. That is why the financial services industry was supportive of the passage of H.R. 3523 which, if enacted, offers additional protections to the confidentiality of shared information. We recognize that as H.R. 3523 was debated, legitimate concerns about protecting an individual's information and privacy were raised by several Members of the House.

As you consider future cybersecurity legislation, however, we do urge you to consider solutions to allow sharing of this type of information under certain circumstances in a manner that protects individuals' privacy rights, but also facilitates their financial protection.

There are legitimate reasons to share this information that benefits citizens. Sharing details about breached customer information and sharing it quickly would allow institutions to take action to prevent fraud against their commercial and retail customers.

In closing, again, please accept my thanks for the opportunity to testify today. Cybersecurity is a vitally important issue for both the private and public sectors. Protecting companies, customers and infrastructures that support our economy is crucial. We commend the subcommittee for recognizing the importance of this subject and for your attention in the strengthening of the Nation's cybersecurity.

[The prepared statement of Mr. Smocer can be found on page 82 of the appendix.]

Chairman GARRETT. Thank you.

Mr. Weiss, you are recognized for 5 minutes and welcome.

STATEMENT OF ERROL WEISS, DIRECTOR, CYBER INTELLIGENCE CENTER, CITI, ON BEHALF OF THE SECURITIES INDUSTRY AND FINANCIAL MARKETS ASSOCIATION (SIFMA)

Mr. WEISS. Good morning, Chairman Garrett, Representative Maloney, and members of the subcommittee. My name is Errol Weiss, and I am the director of Citi's Cyber Intelligence Center, which is responsible for collecting, analyzing, and exchanging threat intelligence to protect Citi's customers, our brand, global business operations, and technology infrastructure against threats worldwide.

I am testifying on behalf of the Securities Industry and Financial Markets Association on how to safeguard the capital markets from emerging cyber threats.

I will be focusing my testimony this morning on cybersecurity in the financial services sector and what we are currently doing to protect our infrastructure, and most importantly, our customers from cyber attacks. SIFMA supports the goals of the Administration and Congress to limit cybersecurity threats against the American people, businesses, and government through a more integrated approach. The increase in cyber intrusions and cyber crimes in the past decade is cause for great concern.

SIFMA member firms are on the front lines defending against cyber threats to the financial markets, and we take this role very seriously. Consequently, SIFMA members currently comply with a number of stringent laws and regulations on the protection of personal data, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Right to Financial Privacy Act. These laws and regulations are reinforced by regular, proactive review and audited by highly specialized regulators that are supported by the FFIEC, an interagency entity that issues data privacy and cybersecurity guidance and monitoring procedures.

In addition, the financial services sector proactively founded the Financial Services Information Sharing and Analysis Center.

Like Michele and Mark on this panel today, I currently serve on the FS-ISAC board of directors. We recognize that Congress shares our concerns regarding the Nation's current cybersecurity infrastructure.

With respect to our industry, we believe it is important to keep the following five principles in mind: SIFMA recognizes the need for expanded information sharing with government agencies, including greater private sector access to threat data from Federal intelligence and law enforcement agencies; access to threat information must be administered in a manner that can provide broader cybersecurity protection without compromising ongoing investigations or the privacy of individual Americans; government agencies should leverage the existing ISACs and DHS US-CERT to facilitate two-way and cross-sector public-private information sharing that will help financial institutions better protect themselves and ultimately protect our customers; and our current regulators are best suited for designating or regulating critical infrastructure.

The Treasury Department, as our sector-specific agency, and the regulatory agencies, through the Financial and Banking Information Infrastructure Committee, should determine what is considered critical infrastructure. A one-size-fits-all approach is not the right regulatory solution. As the amount and sophistication of cyber attacks increases, the need for new technologies, expertise, and talented personnel to combat these threats becomes paramount. Our Nation's universities must focus on developing the next crop of talented information security professionals so that the financial services industry and the Nation can adequately protect itself from cyber attack.

Because cybersecurity is a global problem, and cyber crimes frequently occur across borders, cooperation with international partners is critical to preventing, investigating, and prosecuting cyber crime. The United States should seek strong cooperation with foreign governments to improve cybersecurity and punish those that are responsible for cyber crimes.

SIFMA believes a single uniform Federal breach notification standard would reduce administrative oversight, establish clear notification guidelines, and most importantly, reduce customer confusion. We have played a leadership role in developing policies, procedures, and technology to protect customer data, and we look forward to maintaining that role as the Nation upgrades its cyber defenses. Thank you, Chairman Garrett, Representative Maloney, and other members of the subcommittee for this opportunity to testify today on behalf of SIFMA.

[The prepared statement of Mr. Weiss can be found on page 90 of the appendix.]

Chairman GARRETT. I thank you.

Mr. Woodhill, welcome. You are recognized for 5 minutes.

STATEMENT OF JAMES R. WOODHILL, ADVOCATE, GOVERNMENT AND PUBLIC RELATIONS, YOURMONEYISNOTSAFEINTHEBANK.ORG

Mr. WOODHILL. Thank you. Mr. Chairman, Vice Chairman Schweikert, Congresswoman Maloney, and members of the subcommittee, when I asked how to be a good witness for you, my good friend Billy Tauzin, former chairman of the Energy and Commerce Committee, told me that I needed to do two things: be brief; and then be gone.

But before I am gone, I should tell you what the problem is and offer you at least one decisive solution. Thank you for the opportunity to testify before you today on behalf of the victims and potential victims of corporate account takeovers.

My name is Jim Woodhill. I am a serial entrepreneur in the information security space. I was recruited in December of 2009 to be the advocate for the victims of this new and fast-growing cyber crime by Gartner Inc.'s Avivah Litan, the most prominent analyst in the space.

I am here today because your money is not safe in the bank, not if you are an American church, school district, small business, or political campaign fund; not if you bank online using Microsoft

Windows. Many of you on this committee have heard from victims in your districts.

The shocking thing to victims is that their organizations being vulnerable is an official financial services industry policy known as shared responsibility, your personal accounts are safe, protected by Federal Reserve regulation E, but the status of commercial accounts has been the subject of dozens of lawsuits over State law. The consensus of cyber law experts is that shared responsibility will not hold up long term.

Today, there have been over 500 victims, and at least $100 million has been stolen. Sometimes, the bank makes full restitution, and sometimes, it reaches a settlement with the losses split with the victim. But in hundreds of cases, the bank has evoked shared responsibility and stuck the victim with the entire loss. More than one bankruptcy has resulted. The latest lawsuit was filed on May 17th by TRC operating company, a California energy producer. No matter whose pocket this money comes out of, the stolen moneys are funding enemy R&D. The thefts must stop.

This crime wave did not have to happen. The regulators issued guidance in October of 2005 that would have stopped the crime. Even back then, necessary solutions were expensive to acquire and operate, quickly implemented, and enjoyed wide customer acceptance. But they weren't adopted in great numbers, so that regulators issued much more detailed supplemental guidance last year.

If the solutions were available and the regulators had told the banks to use them, why did United Security Bank sign up last month to spend more on lawyers to defend the lawsuit than the $300,000 it would cost to reimburse TRC?

The answer is simple. America's small and medium-sized banks still have not gotten the memo. Why not? Examples from medicine and public health show that even when life and death are at stake, it takes 20 years to get new information through a medical specialty. As for educating the general public about infectious threats well enough to stop them, public health experience shows that it just can't be done.

Fortunately, account takeover can be stopped by the processors, the 13 big and smart organizations that actually run online banking on behalf of their 5,000 small clients, just as it has already been stopped by the very largest banks who are their own processors.

Weighing alternatives, moving the risk of this crime and responsibility for stopping it to the processors is the victim's first choice if fast government is not in the loop. But there are other solutions that would work. If banks were required to fully disclose the risks of online banking, then those customers moving online could either accept those risks, turn off online banking or move their accounts to where they are safe. I think banks would quickly turn to their processors for protection rather than admit that money is not safe in their bank.

Another alternative is that if fiduciaries of public funds, taxpayer money like city and State treasurers simply refuse to risk taxpayer dollars by depositing them in banks with any history of unreimbursed losses, then those banks would do the same thing.

Regulation E could be extended to all accounts, but I oppose this because disclosure or public fiduciary action would accomplish the same thing and is more free-market-oriented.

Whatever the Congress does, we urge you to do it soon, before there are more victims and more trust lost in the banking system. We must work to make cyberspace a safe neighborhood. Thank you for inviting me to testify.

[The prepared statement of Mr. Woodhill can be found on page 100 of the appendix.]

Chairman GARRETT. Thank you also for your testimony and for being with us today. I thank the entire panel.

We will turn to questions, and within my 5 minutes, I will start from the left and move down as far as I can go.

Ms. Cantley, you note in your testimony that one of the recommendations deals with the issue of making changes to the suspicious activity report. Can you briefly dig into that a little bit and say what changes need to be done there?

Ms. CANTLEY. Yes, sir, and I would add that those have already been implemented by FinCEN. FinCEN has already implemented the recommendations from the account takeover task force. When we looked at the suspicious activity report that financial institutions are required to file, we noted that account takeover was not clearly labeled as a form of suspicious activity, and we recommended to FinCEN that it be appropriately labeled, and that has been accomplished as of the end of last year.

Chairman GARRETT. So what is being done with that information then?

Ms. CANTLEY. Now, when financial institutions have a situation of account takeover and they reported on the suspicious activity report, then FinCEN can use that to do their analysis and also—

Chairman GARRETT. What did they do before they had that little check-off box?

Ms. CANTLEY. I beg your pardon?

Chairman GARRETT. What was being done before you had a little check-off box?

Ms. CANTLEY. Before that, it was not clear what was the method of attack, Mr. Garrett. And so we felt it was appropriate that the industry, through FinCEN, could reflect the volume and size of account takeover appropriately and we felt the suspicious activity reporting process would be a good method for that.

Chairman GARRETT. Okay, thanks. Mr. Clancy, and actually others might want to chime in on this—there is talk in the testimony of you and others with regard to the sharing of information between institutions and the government as well. In order to do so, you have to have a high level of trust there and usually in life, you want to earn trust before you execute on it.

Do you want to briefly talk about ways to do that, to evidence the trust and to enhance ways to share that information between the levels?

Mr. CLANCY. Thank you, Mr. Garrett. Trust, as you mentioned, is slow to build and fast to be lost. The way we have looked at it in the financial sector is we started with anonymous reporting through the FS-ISAC where you can essentially remove the details of who was impacted but give the facts so that others can take action based on those facts.

With that community, there are some limitations. And what we saw as we did this is we started to get a small volume of activity, but when a core, small group of us got together who knew each other socially, knew each other professionally, and we started saying, here is what really happened with that report that we made, the greater richer context came out. And we built what we called a concentric ring model where we had people who were in the center, most who started out with one-to-one personal relationships, we expand that network, that community shares with full attribution, that is what happened to me, this is what we did, this is what we didn't do, we distill out details of that, and honestly, share the broadest community in our sector and build those rings.

Now, what we have done is we have built additional rings so we have started in 2011 an inner circle, if you would, called the Clearinghouse and Exchange Forum which is a subgroup of people like myself and Mr. Graff who are in the capital markets side of the industry and sharing information about attacks on us.

As you get to know the people you are sharing with, you bring more people into that network and the network grows. It is a little bit like social media; the more friends you have, the more friends you get.

Chairman GARRETT. I have a bunch of questions, I have to get them all in.

Speaking of social media, Mr. Graff, I read in the paper that there was a big thing with Facebook the other day. Do you want to just briefly, since you are here, tell us in your information that you have with regard to that transaction and that was reported: What the problem was, was there any cybersecurity aspect to that whatsoever, what is being done to make sure that doesn't happen again, and have the people involved been taken care of?

Mr. GRAFF. Yes. Thank you, Congressman.

As I think you note, my expertise is in cybersecurity and not in the trading systems, but what I know is that the Facebook IPO showed us a design flaw in the methods that are used to operate the IPO. It was a design that has been used successfully for years. Now, we have engineered a fix for that design. We are also taking a look at the processes we use to develop a software and test the software to see if we can improve those.

In terms of cybersecurity and any potential involvement with the Facebook IPO, based on the information I have, which is substantial, there was no cybersecurity element in that IPO.

Chairman GARRETT. Thank you. I have additional questions, but my time has expired. I will now yield to the gentlelady from New York.

Mrs. MALONEY. I would like to ask Mr. Smocer or really anybody on the panel, when there is a cyber attack, how do you find out about it? Do your customers tell you about it? Does your internal division tell you? Does government tell you? How do you find out about it, and then what do you do? Do you report it to government so we are coordinating? Do you report it to other companies? How does it work now? We are hearing that half of the small and large companies are being attacked. How do you find out about it, and then what do you do about it?

Mr. SMOCER. The short answer to your question is yes, all those sources. The reality is that financial institutions are constantly monitoring their environment for indications of attack. So as Errol would tell you at Citi, and he is on the cyber intelligence side, so I will defer to him in a second here, but there are significant investments in monitoring tools to look at the environment to determine if there are attacks under way.

Mrs. MALONEY. These tools that you put in place, are they standards that are required by government? Are they standards that the private sector is putting in place? Are there any required standards? How are these standards being put in place? What are they? Are some companies going far above that with new technologies to protect this information?

Mr. SMOCER. The primary standard that is in place is an expectation from the regulatory agencies and it is within the GLBA, as well, the Gramm-Leach-Bliley Act, to have a strong risk assessment and risk management process in place.

Regulation typically does not specify the exact tools that need to be used, and that, I think, is good because it recognizes that the environment is evolving fairly rapidly and the tool that worked yesterday may not work tomorrow. So it is largely up to the financial institutions to determine their best risk management practices.

But I would quickly add that through the collaborations that we talked about earlier and frankly, most of us at this table have worked together over the last 5 to 10 years in terms of collaborative efforts, we do go through the process of identifying best practices that we would use and share information on tools that have been effective and try and enhance the industry beyond just our own institutions, and I will let Errol comment if he would like to.

Mr. WEISS. Actually, I think you answered that really well.

Mrs. MALONEY. Thank you. I would like to ask Mr. Clancy from the Depository Trust & Clearing Corporation, you mentioned that three of DTCC's subsidiary companies have received notice from the FSOC that they are being considered as systemically important financial market utilities under the Wall Street Reform Act, and recognizing that the new risk management standards for the FSOC designated end user is still being developed, what is your expectation about the extent to which these standards will address information security issues?

Mr. CLANCY. I thank you, Mrs. Maloney.

My expectation as it relates to the FSOC is their focus is very much on the financial aspects, so market risk, liquidity risk, and the like. It is uncertain to me whether or not they will delve into some of the cybersecurity issues. Those are substantially held in the existing frameworks that our regulatory agencies such as the Federal Reserve have, so my expectation is that is how it would be addressed.

From a DTCC perspective, we have looked at the risk that those systems pose to the U.S. financial system and the global financial system and have been working to elevate our level of control and mitigation against those types of threats.

Mrs. MALONEY. In a general sense, when a cyber attack occurs, do you tell your customers, or if private information is extracted on some of your clients, what is the standard that you have? I guess, Mr. Weiss, informing people but keeping it private, how do you address this? Are there laws requiring any disclosure? Or what exactly happens?

Mr. WEISS. Absolutely. If there is a breach of personally identifiable information, there certainly is regulation that requires us to provide that notification to customers.

Mrs. MALONEY. And just basically, what are the three things we have to do to make our country more secure? It is very unnerving to me to think that there are individuals and countries that have entire desks devoted into getting into private information in our financial markets and elsewhere, and what are the steps that private industry is taking to protect this, and I guess, Ms. Cantley, you play a key role in the coordination with government, how is that coordination working? Can it be improved on? How can we do better at protecting our companies, our individuals, and our country from this type of attack?

Ms. CANTLEY. Thank you for that question.

First off, we do have a high amount of public-private information sharing as has been noted in the oral and written testimony. I think we can do more. We would like the government to share more threat indicators that they have with us on a timely basis so that we can act on those and prevent cyber crime in our industry.

We also would like to be in a position to share information safely with the government without having to go through the scrubbing steps so we would appreciate the opportunity for that to be exempted from the Freedom of Information Act. We would like some work done in the telecommunications industry. Currently carriers are required to, by law, deliver everything to the end user.

The government we know knows that some of the traffic that is on our networks is malicious, and if they could give that to the telecommunications carriers, and they could be in a position to drop that traffic before it would be delivered to the end-user, then I think that would be an appropriate step forward.

And then lastly, again, working internationally on legal and diplomatic levels so that when we say someone is a criminal, that individual is arrested, tried, and appropriately sentenced. Thank you.

Mr. GARRETT. I thank the gentlelady. And the gentleman from Arizona is now recognized.

Mr. SCHWEIKERT. Thank you, Mr. Chairman. This is one of those occasions where it is an area of great interest, and there are a thousand questions and about 4 minutes and 50 seconds to ask them.

First, let's say Citi or a major institution, a regional money center bank is finding its systems under attack, someone is trying to somehow go up and down, how quickly does that get shared with others? Do you share it through government? Do you share it through the industry? Do you share it through the working groups? How quickly does that information get disseminated?

Mr. WEISS. Actually, it gets shared very rapidly. It is not automated; there are humans who need to create the e-mails and messages, but it does happen very quickly. So in that case, through the

FS-ISAC and the techniques and the trust that Mark and others talked about earlier about developing this over the past decade, we have been able to create the central rings of trust and to share that information quickly—

Mr. SCHWEIKERT. But you hit on an important point there. Many of us have in the back of our head that there is an automated notification system saying hey, we are seeing this type of malware pinging our systems, boom, and that is electronically shared over some of the security centers. That is not how it works.

Mr. WEISS. It is the first steps that we have taken is really to manually share that information, build that collaboration, and develop the threat indicators so we can share it with the broader audience and help protect our membership at large.

We have recently taken steps in the past, literally in the past year, to build on automated methods so that we can share that information at network speed and protect ourselves at network speed so that we can take the humans out of the loop and get there. It requires significant investment and a lot of work to get there, but we have started that journey.

Mr. SCHWEIKERT. To that point, how quickly is it moving?

Mr. WEISS. It is moving, but again, it is going to take us time to get there. I don't have an answer as to when. I will get back to you.

Mr. SCHWEIKERT. From some of the different organizations you spoke of that are out there, is this one of the areas they work on, automating the notification and the warning systems, and also it is not only the warning but here is the way to block the attack?

Ms. CANTLEY. Yes, there are systems that exist today that do that automated blocking and many institutions have those in place across multiple sectors. What Errol is talking about, and what the FS-ISAC is driving and working with, the U.S. Government again is coming up with a standard template for that information so that it then feeds the systems that exist today and will come down the path.

So we actually have a subcommittee that is addressing that taxonomy to move it forward. As Errol mentioned, though, that is going to require a capital investment, and this is one area where I think the government could assist us because we would like to cooperate together in moving that forward faster.

Mr. SCHWEIKERT. And this is for anyone who would know the answer: How is the technology disparity between a money center institution, a financial trading platform, and my local community bank? How far behind are—is the local community bank more flexible? Are they more exposed? What do you see out there across the financial world?

Mr. GRAFF. If I could, Congressman, let me try to address that.

One thing I would like to—the point I would like to make is that, effectively, all the systems represented at this table, and, in fact, that systems that help Congress, they are all under attack all the time at some level. In contrast to the situation just a few years ago, today Internet attacks are a little bit like weather. We have a little bit more rain or a little bit less rain, sometimes there is a hurricane that comes at us, but, generally speaking, they are all under attack.

I think, to get to the point of your question, the larger institutions that have more sophisticated staff typically will be less susceptible to sophisticated attacks. I think the smaller institutions, the local community institutions are at a disadvantage when it comes to defending against extraordinary attacks that perhaps have taken years to develop. And this is an area where government could assist, I think, quite effectively.

Mr. SCHWEIKERT. And is there infrastructure within, sort of, your organizations for that data information, solution fix, patch fix, to be quickly disseminated all up and down that food chain?

Mr. CLANCY. There are two points. There is the dissemination piece, which I think groups are working to facilitate; then, there is the consumption piece. And what we found through the GISF program is that even for the large, complicated institutions, we had significant problems consuming threat data at the volume and frequency at which it arrived. That is going to be a big challenge for small institutions because they have one or two people who do this stuff, not—

Mr. SCHWEIKERT. And, therefore, the need for sort of an automated platform—

Mr. CLANCY. Correct.

Mr. SCHWEIKERT. —that builds the model.

Mr. CLANCY. And the service provider route, whether it is the telco or the firms that provide those institutions their financial products, are good ways to do that.

Mr. SCHWEIKERT. Mr. Chairman, I see I am out of time. I look forward to another round. Thank you, sir.

Chairman GARRETT. Thank you.

The gentlemen yields back. The gentleman from Massachusetts, Mr. Lynch, is recognized.

Mr. LYNCH. Thank you, Mr. Chairman. And I want to thank our witnesses for attending and helping this committee with its work.

One of the other hats I wear is I am the co-chair of the Task Force on Terrorist Financing and Nonproliferation, so I work a lot with FinCEN, the Financial Crimes Enforcement Network. They do a terrific job on our behalf internationally, on behalf of Treasury and the American people. And they have done a good job, but they are working in a more limited environment than all of you.

If—first of all, I want to try to understand. I know that the exchanges where you have more resources than some of these smaller institutions that Mr. Graff was talking about to protect themselves, where are we in terms of where we need to be with some of these smaller institutions, some of these local banks?

We, as government, have put out there certain benchmarks where we want there to be minimal—at least minimal coverage and protection for some of these smaller institutions. But is that enough? Do we need to do more to require those smaller institutions to provide greater protection to their customers?

And is there also a delta in terms of what we require the exchanges to do and where you think we need to be? Perhaps you do even more; I am sure that most of the big exchanges do more than the government requires. And so, I am trying to get a fix on where we are with the smaller and larger institutions and where we need to be.

Ms. Cantley?

Ms. CANTLEY. Thank you.

Speaking on behalf of attempts to address the smaller institutions, the FS-ISAC thinks this is important. Part of our efforts, the last 2 years, have been strictly focused on education, both for customers and the smaller institutions. And we have held a number of seminars there.

Another important step that we took, because we think it is critical to deal with the fact that most of these small and medium institutions use the same processors, so we built on the authentication guidance that came out in 2005 and then was updated last year and, actually, in some of our recommendations, got even more proscriptive to the service providers on, "Here are things that you need to provide in your products that your institutions can take advantage of."

I would also like to point out to the committee, though, that I don't think additional regulation is the answer to this problem. I think the guidance that we have from the FFIEC is very good and it is applicable to all institutions. And it provides a method for dealing with these attacks in cost-effective means for financial institutions of all size.

Mr. LYNCH. What I am trying to get at is, I am reading the New York Times here this morning, and it has a front-page story about how the President has accelerated and amplified the cyber war that we are having with Iran. And as Mr. Graff has pointed out, this is an incremental thing, where it is ongoing, there will always be these attacks. Sometimes we have a shower, and sometimes we have a hurricane.

What I am concerned about is that a state actor or a quasi-state actor could bring a significant part of the economy down or the financial services sector down, and that would cause great havoc at any time but especially right now where we are trying to build up a recovery.

And are we anticipating that? Are we meeting that challenge?

Mr. Weiss?

Mr. WEISS. Yes, Congressman Lynch, I think one of the basic tenets of the FS-ISAC has been that we recognized a long time ago that all of the institutions in the banking and finance sector were elements of the chain and any one of those chain links represented a potential weakness. And one of the major tenets there was to be able to share incident information and share threat and vulnerability information with all of those members so that they can better protect themselves. And so that was, again, one of the basic tenets that we set out a long time ago to help those institutions, all the institutions.

Mr. LYNCH. Thank you.

Mr. Graff?

Mr. GRAFF. Yes, Congressman, a couple of quick points.

One thing that I think would move us toward the situation you would like to see in terms of preparedness is more cooperation from computer manufacturers and software vendors in producing products that are perhaps easier to secure. And I say that as someone who used to work for a software manufacturer and computer vendor years ago. I have been beating that drum for a long time. There are a lot of issues, and it is a knotty problem. But I think if we make the systems with fewer vulnerabilities to begin with, then especially the smaller banks and other financial institutions would find themselves better placed.

I also want to just point out quickly, in addition to information sharing, which is paramount, we don't have time for a lengthy discussion, but the supply chain problem, the threats of a supply chain attack are really, I think, perhaps the knottiest problem, the most serious issue that faces us, and the one that would be most susceptible to help from government. I have been working on it in the classified government sector for a long time, and I think it is one where the U.S. Government really could provide the most assistance.

Mr. LYNCH. Thank you. That is really helpful.

I yield back, Mr. Chairman.

Mr. SCHWEIKERT [presiding]. Chairwoman Biggert?

Mrs. BIGGERT. Thank you, Mr. Chairman.

And thank you all for being here. I have a couple of questions I hope I can get in.

First of all, maybe, Ms. Cantley, you did address this a little bit, but I have a constituent who called several years ago, a CPA who had her own home business. She kept getting hacked into, and she kept trying to find the software. And it became very costly just for software. She would put another software in, and then she would be hacked again, and on and on.

So what are some of the cost-effective measures that small businesses who do personal financial transactions online or via their smartphone, how can they minimize the risks of threat?

Ms. CANTLEY. Specifically with customers who are using laptops or work stations to conduct business, small businesses, one of the recommendations that our industry has made to these customers is you can use a dedicated computer that you do not use for surfing the Internet or checking e-mail. The price of hardware and software has come down significantly, that this is a cheap insurance way for ensuring that you are save online until, as Mr. Graff pointed out, the industry can get to the point where some of the software in the supply chain is more robust.

But also, I would like to commend companies like Microsoft who have stepped up to the plate and are now producing software that can remediate millions and millions of customers who are infected.

Specifically, to the second part of your question, smartphones and other mobile devices are an emerging risk. And everyone at this table is listening to what is happening in other parts of the world and making sure that we are analyzing those threats and putting appropriate remediations in place and also working, again, on the education front to let people know of the risk there.

The guidance that we have from the FFIEC, while it does not mention mobile phones, is applicable to that technology. So, again, no more regulation or guidance is needed there. We have what will work today, and, as the threats change, I anticipate that we will get additional guidance there.

Mrs. BIGGERT. Okay.

Then, are any of you familiar with ChicagoFIRST? This was something that was founded in 2003 by Chicago-area financial organizations, and it was to enhance the resilience of the Chicago financial community and critical infrastructure overall. And they have held a number of exercises exploring the threats, including cybersecurity threats, and focusing on preparedness.

Mr. Clancy?

Mr. CLANCY. We are very familiar with ChicagoFIRST. They are what we call a regional coalition. So in the Financial Services Sector Coordinating Council (FSSCC) and the FS-ISAC, we partner with organizations like ChicagoFIRST. In fact, my institution, even though we are not based in Chicago, participated in a few of their exercises. And so, that community is one of our circles of trust.

Mrs. BIGGERT. Great. Thank you.

And then one more question. I think we worry about the government agencies adequately protecting the proprietary information of companies that voluntarily share security threat information. And the members of the European Union and the United States are in discussion about this, particularly as it relates to the G-SIFI banks or other financial firms, including insurance.

Have any of you or your organizations been involved in these discussions with the United States and the international regulatory and standard-setting bodies?

I guess I will have to seek the answer to that later on.

Ms. Cantley, how does a small business entrepreneur—where do they go to get the information that they need? Is there a place online where they can go?

Ms. CANTLEY. Yes, ma'am. Many financial institutions have information on their Web sites or they have held seminars for their customers.

Also, the FS-ISAC, through its account takeover task force, has put together a number of joint bulletins which we have made available to our members. They can simply print those off and give those to their customers. And they include all the recommendations that we have for both consumers and businesses for operating safely in the online space.

And then, as Paul Smocer mentioned, StaySafeOnline, which is a Web site that has a number of good recommendations.

Mrs. BIGGERT. Thank you.

I yield back.

Mr. SCHWEIKERT. Thank you, Chairwoman Biggert.

Mr. Dold?

Mr. DOLD. Thank you, Mr. Chairman. I certainly appreciate the time.

Ms. Cantley, again, I am going to go to you first. And I certainly appreciate and agree that I am not sure we want additional regulations, but we are concerned, obviously, about cyber threat and trying to protect consumers, as well.

So I guess my question to you is, what role should the government take in combating the attacks on the private sector or in private systems?

Ms. CANTLEY. I think the key role that we are looking for from the financial services industry is that information sharing on a timely basis as unrestricted as the government can make it so that we can act upon it to protect our customers. And if the government has information about foreign actors as well as software vulnerabilities, we would like to be made aware of that.

Mr. DOLD. How quickly would you like to be made aware? What would be a timeline or a timeframe that you think would be appropriate?

Ms. CANTLEY. As soon as they know about it, sir.

Mr. DOLD. Mr. Graff, I know you talked in your testimony before about—and I had mentioned before—there are hundreds of thousands of attacks that happen on financial institutions each and every day. You equated it to the rain. You equated it to somebody ringing the doorbell. I am not so concerned about somebody ringing the doorbell; I am concerned about somebody taking a crowbar to the side window or somebody going into the backdoor.

So can you talk to me a little bit about how, for instance, the NASDAQ, you identify these threats that are coming in? Obviously, they are multiple and, obviously, at different sophisticated levels. What are you doing at NASDAQ to try to identify these?

Mr. GRAFF. Yes, I would be happy to, Congressman.

There are several ways to answer that, to approach that problem. I think one of the important steps is to become as aware as possible of who the potential actors are and what the most sophisticated attacks are that are out there. So we are very much interested in the kind of information sharing that we have been talking about today. So, information—first, we try to acquaint ourselves with who is attacking various financial institutions, to the best that we know or the best that the FBI can find out, and what tools they are using.

Another approach is to try to build systems that can withstand, to use your analogy, the attack of a crowbar. We put a great deal of effort in to make sure that the critical systems are deeply isolated and are completely inaccessible to anyone coming from the outside except through very, very specific and very highly protected and regulated, specialized channels for the use of exchanging trading information. So one of the things we do, then, is to only allow a very narrow channel of communication into the trading systems that goes through several barriers that inspect it for appropriateness.

And, for example, here is a point that may not be obvious. When you are talking about regulating information that flows to a network, there are two main ways you can do it. One is to constrain where the information comes from. We would call that the IP address, to be technical. And another way is to constrain what kind of information comes through. We could talk, therefore, about the network port it comes through. Firewalls do that both ways. We use several layers of firewalls to put the information that flows in and flows out through continually smaller and smaller filters to protect ourselves that way.

Another point I would like to make in just a moment is that, if we think of the analogy of trying to protect inside our houses, our families and any precious items we might have, it is not necessary all the time to understand all the many ways somebody might try to get into the house. In many cases, the defenses we build are proof against many, many different kinds of attacks, even those we haven't yet anticipated. So we try to build as strong a ring of defenses as we can to make sure that we can defend successfully against unanticipated attacks as well.

Mr. DOLD. From each of your perspectives, I would be interested to find out, as we look at things that we are working on in the committee, what do you identify as the greatest threat that you are trying to deal with right now? And how can we in the Financial Services Committee in the United States Congress help by drafting legislation or highlighting some of the issues that are out there today? What do you view as the greatest threat that you are trying to deal with right now in terms of cybersecurity?

Mr. Weiss, let's start with you.

Mr. WEISS. I am going to go back to one of my tenets and really push on the international cooperation and essentially going after the bad guys and really getting the United States to pressure foreign governments that, if these governments want to compete, if they want to participate in the global economy, the barrier to entry, the cost of entry for them to participate is they need to demonstrate that they have enacted favorable cybersecurity legislation and demonstrate that they are actively prosecuting and punishing the people who are responsible for these cyber crimes.

If I can get a little more technical, on the other side of the spectrum, the issue that we worry about today, certainly, is the advanced malware that we see today and the prevalence of it and it spreading not only to our customer computers but also now into the mobile space that we have mentioned as well today.

Mr. DOLD. Mr. Chairman, my time has expired. I yield back.

Mr. SCHWEIKERT. Thank you, Mr. Dold.

Mr. Stivers?

Mr. STIVERS. Thank you, Mr. Chairman.

And I appreciate all of the witnesses being here and sharing your expertise with us.

Ms. Cantley, earlier you talked about education and how that can help. Tell me, how much of this problem can be cured by good computer hygiene and good habits versus a much more active defense?

Ms. CANTLEY. The Internet ecosystem requires a lot of players to act to make the Internet a safe place for financial commerce.

Certainly, good computer hygiene is important. And Representative Maloney mentioned the Symantec report we have—consumers and business customers who don't patch their computers and aren't even running antivirus software, much less antimalware software. So that is critical. So we have to get the message out to people that that is an important step.

And then the industry, telecommunications and financial, have a part to play, as well as the software manufacturers, there.

Mr. STIVERS. At what point, Ms. Cantley, to follow up, at what point will the industry determine that they can't allow consumers who don't run antivirus software and maybe malware software to connect to your institutions and perform transactions?

Ms. CANTLEY. That particular step, to interrogate a customer's computer, to do that requires agents that an institution would have to put on a customer's computer so that some institutions may choose to go down that road to make that decision.

What I would say is to go back to the guidance that we have from the FFIEC that says, look at layered security, look at what you are doing to validate. Is that the customer at login? Do you think that customer is doing that transaction? And is this transaction in keeping with that customer's pattern of behavior?

So there are things that we can do without necessarily looking at the wholesomeness of that particular customer's computer.

Mr. STIVERS. Great. Thank you.

How many companies—and I guess this is probably for Ms. Cantley and the gentleman from BITS and maybe others who want to answer—use cyber insurance to help protect against liability? I know it is still in its infancy. What percent of folks out there use that?

Mr. SMOCER. I don't have a specific answer. We can probably get back to you.

As you noted, it is in its, I would say its second infancy, because there was some talk about it a decade or so ago, and I think it had some issues. But I think it is growing again. I think institutions are looking at it, but I don't have an idea on the number specifically or a percentage.

Mr. STIVERS. Since it didn't really come up in anybody's testimony, does anybody believe that cyber insurance can be an important part of creating essentially new requirements on folks without laws that we would pass, but a much more dynamic model to ensure that risk management is approached in a smart way, like it is done on workers' comp and many other issues out there?

Mr. SMOCER. I would answer that in the sense that I think it could be helpful particularly in other sectors that may not be as regulated or may not pay as much attention to cybersecurity issues. I think it could be helpful in terms of, obviously, the underwriting, forcing some improvements in the process.

Mr. STIVERS. Thank you.

Several of you have mentioned the CISPA, the Cyber Intelligence Sharing and Protection Act. Does it allow you to share or the government to share information about risks with you in a way that you think happens soon enough or efficiently enough? And I know that it is not completely passed yet, but in its current form. And are there changes any of you would recommend to that bill?

Mr. WEISS. Congressman, what I would say on that one is that we certainly, as an industry, support any improvements that we can make to the public-private information sharing that is happening today. We have some great examples of it, but we can certainly use more of it.

And taking advantage of things like the private-sector clearance program through DHS, for example, is another one to help get access to even more information from the intelligence agencies. But things that we can also do to enhance information sharing even between entities within the private sector that are currently either perceived or real barriers, from a legal perspective, that are preventing some of the information sharing from happening today, we think that legislation could address those kinds of issues as well.

And then, we also would like to see the existing ISACs that are working well—for example, we have talked a lot about the FS-ISAC here today that has over a decades worth of trust-building. We would like to see that those continue to be leveraged and not place any other additional hierarchy or any other essential clearinghouse of ISACs above that, that could potentially introduce more bureaucracy to it.

Mr. STIVERS. Thank you.

Mr. Chairman, my time has expired.

Mr. SCHWEIKERT. Thank you, Mr. Stivers.

Mr. Neugebauer?

Mr. NEUGEBAUER. Thank you, Mr. Chairman.

My subcommittee had a hearing a few months ago on the Office of Financial Research (OFR), which is this new entity that was created under Dodd-Frank to basically put as a clearinghouse or a storing house for a lot of financial data. And I was looking at some of our panelists today, and probably many of you are going to be providing some of that information.

Mr. Clancy, what kinds of connectivity and what—one of the concerns we had—and this question came up during our hearing—was how secure is all of this data that the OFR is going to be mining from the financial markets? Can you kind of elaborate on your discussions with OFR and whether you have concerns about their ability to protect that data?

Mr. CLANCY. Okay, and I am going to focus my comments on the protection as opposed to the disclosures made by OFR.

But the protection—OFR, as part of Treasury, will fall under the Federal Information Security Management Act (FISMA) and they will have cybersecurity standards that will apply. Right? That is kind of the macro picture.

The more brass-tacks view of it is, we have to work out ways to securely send the information that protects the information while it is in transit. The methods being used today are somewhat ad hoc, mainly because of the newness of OFR as an entity in that function. So that is an area that we need to work on.

And then I think they need to look at, from a risk-assessment perspective, the interest of other parties, including other nations, to getting into that data and defend it to that level of aggression.

Mr. NEUGEBAUER. Thank you.

Mr. Graff?

Mr. GRAFF. You put your finger, Congressman, on what I think is a central problem, which is, how do we share that information securely? And there are fairly sound methods I could talk about to protect it in transit. It is a challenge, but the technology is there.

I think the more intense concern might be protecting it once it has arrived inside the Federal networks since they themselves, of course, are a very strong target. And that is, frankly, a concern of ours. We always want to work with the Federal agencies to make sure that the information we give them is sufficient but no more than they need and no more specific than they need.

And, also, we like to hear assurances about the way that they protect those internal systems as well. I think that is an important problem.

I am familiar with FISMA. It does encourage good security, but I think there is a lot of room for improvement there too.

Mr. NEUGEBAUER. Mr. Weiss?

Mr. WEISS. I am sorry, Congressman, I am not familiar with that particular regulation.

Mr. NEUGEBAUER. Okay.

I want to go back, then, to Mr. Clancy and Mr. Graff. So, basically, there are multiple aspects of that. The first is the transmission of the data. Second, once the data gets to OFR, how will it be protected? And then I guess the third piece of it and, I think, something that some of the market participants have brought up, is who will then have access to that data moving forward and how will they be able to use that data and access it?

And those are areas that you have some concern in and are certainly—

Mr. CLANCY. Yes. I think access to the data itself is one of the key questions, both in terms of the appropriateness of what is done with the data, how it is used, where it is exported, as well as how you defend against it being misused.

What we mentioned earlier on the panel is accounts are taken over. This happens to institutions and accounts inside. And so if someone at OFR's accounts were taken, access credentials were used, somebody else could potentially exploit the data that exists in those repositories. To that end, we would expect a high level of resilience to those types of attacks to be built into the design and system operation of the platforms used for the data analysis and mining by OFR.

Mr. NEUGEBAUER. Thank you for those comments.

We are talking about market participants that provide financial services, and we are talking about those that use it. But, as well, I was going back to talking about small businesses and individuals, and their computers at home or their laptops. And there is a lot of discussion going on right now about using cloud-type systems to store your really sensitive data rather than storing it on your hard drives.

I guess the question I have is, in your professional opinion, is my data more secure in a remote location or is it more secure on my computer?

Mr. CLANCY. Again, this is a simple example. I have a neighbor who is the CEO of an intellectual-property-based company. His IT group consists of two people. Anything he puts in the cloud will be better defended than he can do it himself. At my institution, however, we have significant skill and expertise and are a particularly interesting target. Our information in a public cloud would probably be very hard to defend with the basic level of service that most of the cloud providers offer.

Mr. NEUGEBAUER. Okay.

Mr. GRAFF. I have to agree, Congressman. I think for the average person, their own home system is unlikely to be safe enough to give them the security they want. And it is a good practice in general, I think, to store that information with people who are professionally trained to do it. And, of course, one also can transfer some liability to them, as well, as they assume responsibility for the data. That is an important factor, too, I think.

Mr. NEUGEBAUER. So these providers have a much more robust infrastructure to protect your data than the individual at home, is that—

Mr. GRAFF. Many of them would, sir, yes.

Mr. NEUGEBAUER. Yes.

I thank the gentleman.

Mr. SCHWEIKERT. Thank you. Thank you, Mr. Chairman.

Mr. Manzullo?

Mr. MANZULLO. Thank you.

I have a couple of questions as to the distinctions, if any, that occur on these cyber attacks. We are talking today about just banking online, is that correct? Or are we talking about accessing 401(k) information? So how broad does this get?

Ms. CANTLEY. Cyber attacks are across our industry, so, yes, they could be going against your checking account, they could be addressed to your 401(k). We have had insurance companies report this. So it is not just that particular isolation.

Mr. MANZULLO. So is a 401(k)—that is identified by a Social Security number, is that correct?

Mr. CLANCY. A lot of the providers used to do that practice and have moved away from it, some of them more aggressively than others. And so the underlying, sort of, database entry is probably based on a Social Security number, but the authentication credentials are based on other data that is selected by the customer.

Mr. MANZULLO. Which means it is not covered?

Mr. CLANCY. The overall account is protected, but they are not using a Social Security number as the user name to sign on.

Mr. MANZULLO. Okay. All right. That answers my question on it.

And then the issue, when at one time you would write a check, take it to a bank, and then not worry about covering it for a couple of days; of course, that has all stopped. It is done electronically now.

What about these electronic transfers, as they were, between banks? Have these ever been hacked that you know of?

Mr. CLANCY. The platforms that perform the transfers have not, but, again, the access to accounts that authorize those platforms to perform a transaction, those front-end systems have been targeted.

Mr. MANZULLO. What about Social Security now that there are mandates that Social Security checks have to be deposited electronically into a person's checking account? Now that you have a Federal mandate, is that covered?

Have there been instances where the Federal Government has gone to transfer a Social Security recipient's monthly check into a checking account and that the money has not showed up before it got into the actual account?

Ms. CANTLEY. I am not aware of any instances of that, sir.

Mr. MANZULLO. Last year, on my e-mail account, someone came in, attacked the account, put out the statement that I was—maybe, Judy, you got it—I was trapped in Britain and needed people to send $1,500. And another Member of Congress, who was a Democrat, called to see if I was okay. I thought that was very generous on his part. But they took all of my addresses and went in there, and I had to reconstruct that.

Is this what we are talking about, or is this more intense than this?

Mr. CLANCY. We have been talking about things that cover that and things at higher intensity.

That particular example is, unfortunately, a somewhat common scam. And what happens is that the access to your e-mail account—you were maybe at a hotel and you signed in, and that had a keylogger and it took your password. And what they are really doing is a technique called social engineering. They are trying to create a context that your fellow Members of Congress might have known you were in London, might have been unrelated to that, and were sympathetic and would then take an action, to send money, that they wouldn't have otherwise done. And that is the underlying technique that these bad guys are using, is that sort of driving your behavior based on provocative messages.

Mr. MANZULLO. Some of my colleagues would have liked me to stay in Britain, not be able to get back on it.

I think the broader issue really is—Secretary Rubin said that he simply does not bank online. Maybe this would be a revival for the post office, if people—no, I am serious. We don't bank online, my wife and I don't bank online, because I have always been sort of old-fashioned and would rather put that stamp on there to get it out.

But, Mr. Woodhill, until you stopped by the office yesterday, I always presumed that even commercial accounts were safe. And you make a reference in here to accounts from Members of Congress and their campaign funds.

How pervasive is this? And should American people really take a look at whether or not it is worthwhile to bank online?

Mr. WOODHILL. Congressman, that is the threat that my victims group is trying to head off, that cyberspace will become such an unsafe neighborhood that Americans will just decide that they can't bank online.

My fellow panelists have made the point for me that individuals and small businesses and your campaign fund can't possibly have the cybersecurity expertise to secure online banking on their end. I further submit to you that if community bankers in your district become cybersecurity experts and spend their time studying FS-ISAC bulletins instead of out making loans to move our economy forward, the bad guys have won even if they don't make off with a dime.

So your money is not currently safe at the bank except at a small number of very large banks, probably Mr. Weiss' for example, that employ multilayer fraud controls and have really brilliant people monitoring them. Otherwise, it just matters—it is whether you are randomly targeted, like your Yahoo account was. The same people who got to your Yahoo account could get, if you had commercial accounts and you were banking from that PC, they could get to your money.

I do like the idea of buying a new PC to do online banking as a stimulus measure. However, as a $500 or $600 tax on our small organizations just for the privilege of using online banking, I am opposed.

Mr. MANZULLO. Thank you.

Mr. SCHWEIKERT. Mr. Manzullo, I would have sent you money if I knew you were trapped in Europe.

Mr. MANZULLO. But there was another one that just came out this past week again.

Mr. SCHWEIKERT. Were you trapped again?

Mr. MANZULLO. Well, no, I am not back stuck in Britain, but this one says, "I have to share with you," this is TV 15. People click on it, and it is somebody selling a product at their house. And I guess the virus that went through again and didn't—I got back, 15 or 20 people saying you have been hacked into. I had answered a friend's e-mail, and I said, "You have been hacked into," but I guess when I answered him, then I evidently picked up the virus myself.

Mr. SCHWEIKERT. Your first mistake: Don't have friends.

Mr. MANZULLO. That is not hard when you are a politician.

Mr. SCHWEIKERT. Ms. Cantley, there are a couple of questions I want to try to run through. One was given to me by the chairman, but one I have a personal interest in. And let's see if I can phrase it the proper way.

A bot, we often—what we do is we will shut down the server. But there is legacy software still—or there is still software, often, out there in the world sitting on computers. And my understanding is, we will have the creative souls who will come in, set up anew, and hijack that. How much is that mechanic, because of the residency on computers around the world, also a threat?

Ms. CANTLEY. I think that is a very large threat. And if you would allow me to defer to Mr. Weiss on this question, because he has been very active on the botnet takedown, sir.

Mr. SCHWEIKERT. Mr. Weiss? And you might want to—am I phrasing it in the proper mechanics?

Mr. WEISS. Yes, that is absolutely fine. And let me just elaborate on that a minute.

So, just to really address that, one of the initiatives that we recently had within the financial services sector that we thought was a very proactive thing to do on behalf of our consumers to help them protect themselves was a partnership with the FS-ISAC and NACHA and others from the financial services sector partnered with Microsoft to go after three of the very dangerous botnets that were responsible for many of the account takeovers that we had in the industry.

Mr. SCHWEIKERT. Now, just one point of reference. When we say "go after," that is actually at the server level?

Mr. WEISS. This was a civil action to go after the command and control infrastructure for those particular botnets.

Mr. SCHWEIKERT. And the nature of my question is what is residency—

Mr. WEISS. Right.

Mr. SCHWEIKERT. —on individual computers and systems.

Mr. WEISS. Right. So what we normally find is that when—we have talked a lot about all these e-mails that people are clicking on. When you click on one, you get infected with one of these variants. It is more than likely that is not the only thing that you have been infected with.

So the thing that we took advantage of with this takedown project with Microsoft was that, now that we have the command and control infrastructure seized from the criminals, those computers are now phoning home or beaconing back to the good guys. So instead of being under the control of the bad guys at this point, those computers are—

Mr. SCHWEIKERT. What you have done is a redirect.

Mr. WEISS. Exactly. And the long-term hope here is that, as we continue to collect forensic evidence, we will at one point be able to clean those machines and get them back under the control of their owners.

Mr. SCHWEIKERT. Okay. Interesting.

There is one question that the chairman wanted me to ask, and he does this quite often. I am going to start with Mr. Woodhill.

Quickly, tell me, if you were going to do one thing, what would it be, in cybersecurity?

Mr. WOODHILL. For my particular crime, we are blessed that it is easy to stop. The solutions are in place, so just move the responsibility, as, actually, Ms. Cantley spoke about, to the processors. She is working with the processors to implement the guidance.

My number one is actually that we have to stop malware. If you look at all these attacks—on the Pentagon, on small businesses, on everybody—at the root of the attack is the fact that computers will run software that other people wrote who are not your friend. And we haven't figured out—the antivirus products have stopped working over 5 years ago. We haven't gotten them working again, and we can't detect the latest-model malware.

Mr. SCHWEIKERT. Okay, so the threats of malware.

Mr. WOODHILL. We have to stop malware.

Mr. SCHWEIKERT. Mr. Weiss?

Mr. WEISS. I would go with, we have to keep the ball rolling on the information-sharing initiatives that we have in place today with the existing legislation that has been recently passed.

Just to give you an example there, in June of 2011, the FS-ISAC became the third of the 18 ISACs to maintain a regular presence on the NCCIC floor with DHS. And from that point going forward, we have had the ability, on a daily basis, to share threat vulnerability information between the sectors, between our partners with government. And we have made great strides in improving the relationship between the financial services sector and our government partners.

Mr. SCHWEIKERT. Okay, so threat sharing.

Mr. WEISS. Yes.

Mr. SMOCER. I would take it one step further and say threat analysis. So, a lot of data flowing back and forth. More could come from other sectors. But taking that data and analyzing it to know when you have the incident that really matters, or, more importantly, when you see the trend that is coming out, that you know you need to act sooner rather than later.

Mr. SCHWEIKERT. Can I say threat analytics?

Mr. SMOCER. Yes.

Mr. GRAFF. I would take a slightly different approach. I am very concerned about, to reiterate, the supply chain problem—that is to say, the possibility that computer manufacturers or other nation-states may actually be able to introduce pieces of hardware or software into computer routers, network servers, even network cables, to be able to manipulate the computers that way, in a way that individual companies really aren't equipped to detect.

And there are methods inside the Federal Government right now in the intelligence sector that are working on this problem. And perhaps if we could get some of the benefit of those—

Mr. SCHWEIKERT. So, expansion of physical barriers. Are you speaking of, like, sonic walls or—

Mr. GRAFF. Yes. It is a problem both in hardware and software, but I think the more pernicious problem is, in fact, hardware coming out of something that appears to be a router but actually has specialized chips in it. Very concerning.

Mr. SCHWEIKERT. Forgive me for going so over my time, but Mr. Clancy?

Mr. CLANCY. It would be very simple. Take the program I mentioned, GISF, which does both threat sharing and threat analysis, and make sure that it continues and expands.

Ms. CANTLEY. And engage the telecommunications industry in this discussion to help.

Mr. SCHWEIKERT. Okay. Can you give me a little more definition there?

Ms. CANTLEY. Yes, sir. Our telecommunications industry, because of the fact that they pass this traffic between us, between our customers and us, and between other sectors, are in a situation in our infrastructure where they see this traffic. And if they were given the authority to dump it, that would get rid of a lot of this.

Mr. SCHWEIKERT. All right. Thank you.

The gentlewoman from New York?

Mrs. MALONEY. Thank you very much.

And thank you to all the panelists.

Last year, the SEC came out with a guidance that financial firms had to disclose the cost of material cyber attacks and include a description of relevant insurance coverage to shareholders.

How common is the use of cyber insurance by financial institutions now? Do they have this type of insurance now? Can someone answer? How common is it?

Mr. CLANCY. It is not very common. And in my institution, the question is, who would insure me against $1.66 quadrillion worth of transactions? That is the challenge.

Mrs. MALONEY. What factors are considered in determining whether or not an institution has a cyber risk?

Ms. CANTLEY. The same factors that are used that are part of Gramm-Leach-Bliley and SOCs and all the other guidelines that we have are used to evaluate cyber risk, and going through that application process.

Mrs. MALONEY. There have been some reports about "pump and dump." I would like to ask those of you in the private sector, what steps has the private sector taken, or Federal regulators, to prevent so-called "pump and dump," these scams where thieves try to move the market by running up the price of a security with buy-and-sell orders in accounts they have taken over? How common is this practice? I have read about it in the paper. Is it common? Is it very uncommon?

Mr. CLANCY. I don't have a sense as to frequency. It certainly happens enough that there has been a group put together that is called the National Cyber Forensics Training Alliance out in Pittsburgh, Pennsylvania, which is a collaboration of private sector entities and law enforcement partners, where information specifically to those types of crimes is shared and then acted upon in law enforcement and then potentially referencing back to activity that is being worked through FinCEN.

Mrs. MALONEY. And I would like to ask Citi, Mr. Weiss, your great bank was the subject of a very high-profile cyber attack in 2011. Can you tell us what changes Citi has made since then to protect your cybersecurity systems? What is different now?

Mr. WEISS. Sure. That breach that you referenced in May of 2011 impacted our credit card operations business only, and no personally identifiable information was disclosed as a result of that breach.

Since then, we have had many lessons learned and we have invested millions of dollars and a lot of people's time to improve the monitoring and detection systems that we have in place today to ensure that kind of a breach does not happen again.

Mrs. MALONEY. Okay.

I would like to ask SIFMA or anyone who is familiar with their practices, SIFMA supports Federal preemption of State laws related to breach disclosures and notification. What specific differences in State laws pose challenges for SIFMA? And can you explain why you favor preemption?

Mr. WEISS. I will take a first crack at that one.

The issue that I think we really have, one of the major ones for us, is being able to reconcile the more than 50 different State laws and local regulations that we have to deal with when it comes to notification. It is a time-consuming process to figure out which ones apply, what notifications we have to provide, when, and how much.

And just the consolidation to a national breach-notification standard that we could rely on would eliminate that administrative overhead, that burden, allow us to turn around these notifications much more quickly, and, we think, end the confusion that the customers are getting today when they receive multiple notifications, different formats, and different remediation standards.

Mrs. MALONEY. I would like to ask Mr. Woodhill: In your testimony, you make it clear that you believe that account takeovers continue to be a challenge at financial institutions. To what extent could regulatory changes address your concerns? Or is legislation—or what actions are needed to address the problems that you perceive are there?

Mr. WOODHILL. Of course, if you read my bio, you would know I am not exactly a fan of regulation.

Mrs. MALONEY. Yes.

Mr. WOODHILL. In this particular case, to stop this crime by a date certain and that be close in, it appears that a small—or actually will reduce the net amount of regulation, because it will take the FFIEC guidance and not make these poor community bankers study it, but, as Ms. Cantley said, put that responsibility, those risks on their processor that is running the IP, that it is a huge organization and has a top security staff now.

In one case, Representative, the bank had the necessary fraud controls in place, was paying for them to the processor, just was unaware of it. They were getting fraud alerts; they just didn't know to look at them. And that bank has spent a million dollars on legal fees to defend the notion that they weren't responsible for transfers that they were getting these red alerts from their processor about.

Mrs. MALONEY. My time has expired. Thank you.

Mr. SCHWEIKERT. Thank you.

Chairwoman Biggert?

Mrs. BIGGERT. Thank you, Mr. Chairman.

Following up on this a little bit, Ms. Cantley, there is a survey that is described in your written testimony which notes that there is a significant drop in commercial account takeovers between 2009 and 2010. To what do you attribute this large reduction in fraud?

Ms. CANTLEY. The answer may surprise you, Congresswoman. When we polled our members with our most recent survey, they said that customer education was the most specific driver to that.

Mrs. BIGGERT. Okay. Any idea about current fraud trends regarding corporate account takeovers?

Ms. CANTLEY. That survey was specific to a corporate account takeover.

Mrs. BIGGERT. Okay. Thank you.

Mr. Smocer, in your testimony, in the list of various committees and information-sharing groups that you have in there, it seems like there might be too many of these groups, each slightly different, so that we might have a lot of information flowing back and forth, but potentially the correct information may never get to the right place.

Is it possible to—should we be streamlining information sharing even as we seek to improve the flow of information?

Mr. SMOCER. I think the answer is probably at two levels. In terms of a lot of the initiatives that we take around best practices and improvements in resiliency, I think we do work very closely together across a number of the organizations and associations that we have. And we do try to make sure that each of us is focusing on key areas and we are not wasting resources in terms of time and effort.

Specific to information sharing, I think within our industry we are doing a good job at the sharing through the ISAC, centering all that information on the ISAC. I think when we start to think about sharing between sectors and sharing between the public and private sector, having some of the standards that Mr. Weiss mentioned earlier in terms of how that data gets formatted, how we can look at it collectively will be important. Because I do think there is a risk that so much data will come in from so many different sources that we will miss the answer in the analysis and we won't be able to do it well.

Mrs. BIGGERT. Thank you.

And then just a quick question. We have been talking so much about what is happening with people who have been hacking in or attacking. And I think, Mr. Clancy, early on you said something about enforcement.

Maybe this is beyond the scope, but how many of these people get caught? Or do they? What happens? What is the penalty, and what happens?

Mr. CLANCY. I don't have a specific answer on how many people get caught. But I think the way to think of the problem is, the attacks happen in a time scale of seconds, minutes, and hours, and the law enforcement activity, while very important, happens on a scale of months and years.

And so I think the challenge that we have as a sector is the difference between those two points and the way you respond to them. The minute, second, hours front, you have to focus on mitigation. Mitigation is stopping an event from occurring, stopping it from expanding, and preventing others from being similarly targeted. And that is why we focus so much on information sharing.

Mrs. BIGGERT. Would anybody else like to—okay.

I yield back. Thank you.

Mr. SCHWEIKERT. Thank you, Mrs. Biggert.

Mr. Stivers?

Mr. STIVERS. Thank you, Mr. Chairman.

My question, I guess, is for Ms. Cantley and Mr. Weiss. Under Regulation E, consumers get third-party liability protection up to—they can't lose more than $50 for unauthorized electronic transfers. And I know some people have talked about expanding that to business customers to help protect small businesses from these account takeovers. That would essentially shift the liability to the financial institutions and potentially, I suppose, make the small businesses less interested in some of their protection, although I guess Reg E does require them to immediately notify, which would maybe benefit the system.

Is that a good idea or a bad idea?

Ms. CANTLEY. Currently, commercial and small business customers are covered in every State by UCC 4A. And we feel that that has stood the test of time in addressing this issue.

Mr. STIVERS. What is the coverage amount under UCC—

Ms. CANTLEY. That the standards need to be commercially reasonable.

Mr. STIVERS. Mr. Weiss, do you want to—

Mr. WEISS. I really have nothing else to add to what Michele stated.

Mr. STIVERS. Looks like Mr. Woodhill—go ahead, sir?

Mr. WOODHILL. If I may, what "commercially reasonable" means as a matter of law has been the subject of 12 lawsuits. Two of them were settling for 100 cents on the dollar just as soon as the bank saw what the judge had to say in its denial of their preliminary—motion for preliminary finding for the defendant. One was actually won, at least so far, by the bank, and one was won by the victim.

The consensus at the big security conference this past spring, the consensus among cyber law experts was that, given the new 2011 guidance, going forward UCC 4A will be found currently to mean that the banks are liable. Our victims group has deep concerns about making small bankers liable for risks that they can't really understand and they can't really manage. So we would like to see those risks and responsibilities moved to these big processor organizations.

Because it is possible that small banks would have to hold additional capital against the possibility that these large, manned accounts might have to do a refund because the big transfers were fraudulent, not going back 90 days. And this is just—this is too much for a small business, too much for small banks.

Mr. STIVERS. Thank you very much.

I yield back.

Mr. SCHWEIKERT. And one last—Mr. Manzullo will be our last questioner of the panel. And I do appreciate your patience, but this is an interesting area with lots and lots of layers.

Mr. Manzullo?

Mr. MANZULLO. Thank you.

I bought a new computer a couple of years ago, and the store recommended "X" company antivirus software. And for different amounts, you got different coverage. Does this stuff work?

Mr. CLANCY. It works to a point. And so, the challenge has been that the attackers innovate, and they run their attack software against the commercial products—all of them, not just the one you bought, but the one that everybody else buys and so on and so forth—and they make sure their attack code is resilient to detection. And so, it is a cat-and-mouse game.

So, on the day that they create the software and send it, does your commercial tool that you bought or even the free tools that you use find it? Very often not. Does it 2 weeks later? Yes, very often it does. So there is this window-of-time problem that is very hard to address, and the attackers will continue to innovate.

Mr. MANZULLO. But it is worthwhile to buy some type of protection?

Mr. CLANCY. Yes. You are much better off with it than you are without it, but it is not a perfect defense.

Mr. MANZULLO. When my account got hacked into last year and my contact lists were stolen, I called a representative from this company—and I don't want to give the name of the company. It is a fairly responsible company; it just wouldn't be fair to name them publicly. But the lady said that because the information on the e-mail account was not stored in my PC but somewhere—I don't know if the word is the "cloud" or wherever else it was, is that this antispyware, whatever it is, was unable to protect it.

You are nodding. Maybe you could explain to me what she tried to explain to me on the phone.

Mr. CLANCY. Sure.

Mr. MANZULLO. What happened there?

Mr. CLANCY. Essentially what happened, most probably—obviously, I am just basing it on what you said—is that the sign-in ID, the username and password you use to get into your mailbox, was compromised, and the bad guy logged in from some other system to that system in the cloud to pretend that they were you to send out these e-mails. Right? Or using a system to do that on their behalf, as opposed to actually attacking your own personal laptop or computer that you were using. And because their credential was stolen, it appeared to that mail provider as you signing in with your password so it must have been you. Right? So the client tool on your PC didn't come into play because it was external to you.

Now, it would have potentially prevented the fact that that sign-in to your e-mail account was taken in the first place if that actually occurred when you were using your computer and not something perhaps when you were traveling or on another machine.

Mr. WOODHILL. But the question is, how did your log-on ID and password get compromised? The typical way is because they had malware on your PC that watched you enter your user ID and password, stole it, and transmitted it to the bad guys to use in that scam.

There are other attack modes, however. You can recover a user ID and password on Yahoo by knowing some challenge questions that they can research about you. So there are other possibilities, but almost always it is malware.

Mr. MANZULLO. The reason I ask the question is that, is it an option to take and download what is in the cloud now directly onto your PC? And would that make it more secure? Or would that—the lady said it would actually open up everything else on the PC to that attack.

Mr. WOODHILL. Congressman, it would make it less secure, because the testimony here among the experts is that you can't secure your home PC. The Pentagon can't secure its desktop PCs. So it would be two places you could be attacked, not just one. And you could lose your PC, it could be physically stolen in a robbery of your house, and then the data would be on your hard disk.

Mr. MANZULLO. The final question is, do you remember—I guess it still goes on, with the robo-calling of the telephones, where computers would generate a list of seven numbers and then actually come up with a combination that it will ring? Do people who do this take a look at somebody's name and then try to figure out different combinations of that? How individual is this in the hacking that takes place? Or is it mostly on a broad base so that everybody gets hacked at one time?

Oh, no, that is not correct because the Crystal Lake School District got hacked and had $340,000, and it was just their district that they hacked into.

Mr. CLANCY. I would say both. There are what we call commodity attacks that are broadly targeted based on an e-mail list that was found, whether your name is posted on a Web site or what not, based on people just trawling the Internet looking for identity. And then there are targeted attacks that are very convincing that are very personalized to the individual. And you have sophisticated criminals doing those attacks and more basic feeder farm team criminals doing the more commodity widespread things. So you have both.

Mr. MANZULLO. So then the Yahoo—my account is Yahoo—or Gmail, whatever it is, you really shouldn't have your name on that address. Would that be correct? Such as "jimwoodhill@yahoo.com."

Mr. WOODHILL. Actually, if you look at who lost money, it is random. Your school district was just randomly unlucky. Every time banks sign someone up like your school district for online banking, they get a kind of reverse lottery ticket, that if their number is selected by the criminals, they lose $300,000, as Crystal Lake does.

And so in studies of the victimization patterns, it doesn't matter if your name is included or not, you are just randomly unlucky to end up with malware on your PC and getting your money stolen. So those kinds of things—the criminals try everything. They try every attack every which way, so you can't defend yourself.

Mr. MANZULLO. Thank you.

Mr. SCHWEIKERT. Thank you, Mr. Manzullo.

And thank you to the panel. This was interesting, and I have the feeling we are going to be spending a lot more time on this subject over the years to come.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection—I am always worried someone is going to walk in and just object at that moment—the hearing record will remain open for 30 days for the Members to submit written questions to these witnesses and to place their responses in the record.

I can almost assure you there were two or three Members up here who had technical questions that will be coming to you.

Thank you for your participation.

This hearing is adjourned.

[Whereupon, at 11:40 a.m., the hearing was adjourned.]

APPENDIX

June 1, 2012

Robert Hurt Opening Statement – Capital Markets Subcommittee Hearing – "Cyber Threats to Capital Markets and Corporate Accounts" - June 1, 2012

Thank you for yielding Mr. Chairman and thank you for holding this hearing today on the important issue of protecting financial systems and data from cyber threats.

We face an unseen and often unnoticed threat to society each and every day. Hackers and cyber-criminals, many of which are state-sponsored hackers from China and Russia, are constantly targeting sensitive government and private sector information for theft or sabotage. These attacks pose grave threats to our national security and American economic prosperity.

Last year, I had the privilege of serving on the House Cybersecurity Task Force, which examined the broad range of issues associated with growing cyber threats and also developed recommendations for how to update relevant laws and policies to enhance the defense of our digital infrastructure.

Given the significant threats that cyber criminals pose to individual privacy and resources, it is critical to protect Fifth District Virginians and all Americans from these attacks. I look forward to hearing from our witnesses about the steps that financial services firms are taking to maintain the integrity of their networks and sensitive data.

Again, I want to thank the Chair for holding this important today and thank our witnesses for their testimony.

Testimony of

Michele B. Cantley

Chief Information Security Officer

Regions Bank

On Behalf of the

The Financial Services Information Sharing & Analysis Center

Before the

United States House of Representatives

Capital Markets and Government Sponsored Enterprises Subcommittee

June 1, 2012

FS-ISAC BACKGROUND

Chairman Garret, Ranking Member Waters, and members of the Subcommittee, my name is Michele Cantley. I am the Chief Information Security Officer for Regions Bank and I am appearing today for the Financial Services Information Sharing & Analysis Center (FS-ISAC). I want to thank you for this opportunity to address the U.S. House of Representatives Financial Services Capital Markets and Government Sponsored Enterprises Subcommittee on the important issue of corporate account takeover and its impact to the financial services industry. In addition, my written testimony includes other recommendations for improving communication between the public and private sector about cyber threats as well as the efforts that our financial services sector can take to improve our defenses and educate our customers.

First, let me provide some background on Regions and FS-ISAC. Regions Financial Corporation, with $127 billion in assets, is a multi-state regional bank and is one of the nation's largest full-service providers of consumer and commercial banking, wealth management, mortgage, and insurance products and services. Regions is the 12th largest U.S. bank by deposits and loans and serves customers in 16 states across the South, Midwest and Texas, and operates approximately 1,700 banking offices and 2,100 ATMs. Regions is a member of the FS-ISAC.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD63) that called for the public and private sector to work together to address cyber threats to the Nation's critical infrastructures. After 9/11, and in response Homeland Security Presidential

Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time the membership has expanded to over 4,400 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, exchanges and clearing houses, payments' processors, and over 30 trade associations representing the majority of the U.S. financial services sector.

The FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council (FFIEC), United States Secret Service, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and state and local governments.

With respect to cooperation within the financial services sector, the FS-ISAC is a member of, and partner to, the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection established under HSPD7. We also work closely with other industry groups and trade associations that are members of the FS-ISAC including the American Bankers Association (ABA), Securities Industry and Financial Markets Association (SIFMA), Independent Community Bankers Association (ICBA), and the BITS division of the Financial Services Roundtable. In addition, our membership includes various clearing houses and exchanges such as the National Automated Clearing House Association (NACHA), Depository Trust and Clearing Corporation (DTCC), New York Stock Exchange, NASDAQ, The Clearing House (TCH), all of the payment card brands and most of the card payment processors in the U.S.

The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that provides anonymity to allow members to submit threat, vulnerability and incident information in a non-attributable and trusted manner so information that would normally not be shared is instead provided for the good of the sector, the membership and the nation. FS-ISAC information sharing services and activities include:

- delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the 24x7x365 FS-ISAC Security Operations Center (SOC);
- an anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information in a non-attributable and trusted manner
- presenting cyber security briefings and white papers;
- operation of email list servers supporting attributable information exchange by various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, threat intelligence sharing open to the membership, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee, Compliance and Audit Council, Insurance Risk Council, and the Payments Risk Council;

- anonymous surveys that allow members to request information regarding security best practices at other organizations;
- bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
- emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS);
- emergency conference calls to share information with the membership and solicit input and collaboration;
- engagement with private security companies to identify threat information of relevance to the membership and the sector;
- development of risk mitigation best practices, threat view points and toolkits;
- Subject Matter Expert (SME) committees including the Threat Intelligence Committee and Business Resilience Committee that provide in-depth analyses of risks to the sector, provide technical, business and operational impact assessments and recommend mitigation and remediation strategies and tactics;
- special projects to address specific risk issues such as the Account Takeover Task Force (see pages 10-13);
- document repositories for members to share information and documentation with other members;
- development and testing of crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies;

- participation in sector, cross-sector and national exercises such as the Cyber Attacks Against Payment Processes (CAPP), National Level Exercise 2012, and the Cyber Storm series;
- semi-annual member meetings and conferences; and
- online webinar presentations and regional outreach programs to educate small to medium sized regional financial services firms on threats, risks and best practices.

A key factor in all of these activities is trust. The FS-ISAC works to facilitate development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations such as law enforcement, regulators, and intelligence agencies. The FS-ISAC, for example, uses a traffic light protocol (red, yellow, green) to indicate to its members how information may be disseminated to FS-ISAC members, partners, and other ISACS. This protocol has been a key component in developing a clear means for trusted distribution of information. The FS-ISAC has also built a model for sharing information without attribution to a specific institution and also uses non-disclosure agreements (NDAs) to ensure that confidentiality of non-public and sensitive information is maintained.

The FS-ISAC is an active participant in cross-sector information sharing and has engaged in a number of cross-sector information sharing programs such as the Joint ISAC BOTNET Mitigation Process Working Group and the Cross Sector Information Sharing Framework, a vehicle for real-time cyber information sharing between the sectors. FS-ISAC currently also has a leadership role in the National Council of ISACs.

The FS-ISAC has implemented a number of programs in partnership with the Department of Homeland Security (DHS) and other government agencies. As part of this partnership, the FS-ISAC set up an email listserv with U.S. CERT where actionable incident, threat and vulnerability information is shared in real-time. This listserv also allows FS-ISAC members to share directly with U.S. CERT. In June 2011, the FS-ISAC, in partnership with DHS became the third ISAC to participate in the National Cybersecurity and Communications Integration Center (NCCIC) watch floor. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. Over the course of a year, our presence on the NCCIC floor has largely greatly enhanced situational awareness and information sharing between the financial services sector and the government. The FS-ISAC recently obtained funding from a member to have full-time staff on the NCCIC floor in addition to the part-time resources that are currently deployed.

In addition, FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG). This group was set up under authority of the National Cyber Incident Response Plan (NCIRP) and has been actively engaged in incident response. Cyber UCG's handling and communications with various sectors following the RSA attack in March of 2011 is one example of how this group is effective in facilitating relevant and actionable information sharing.

Finally, it should be noted that the FS-ISAC and FSSCC have worked closely with DHS, the U.S. Department of Treasury, FBI, U.S Secret Service and other government partners to obtain over 250 Secret level clearances and a number of TS/SCI clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information security threats and have provided useful information for the sector to implement effective risk controls to combat these threats. The FS-ISAC would like to see this process updated to efficiently and effectively provide more clearances to the private sector.

PUBLIC / PRIVATE SECTOR RESPONSE TO THE CYBER CRIME ISSUE

The FS-ISAC is aware through its information sharing arrangements with both public and private sector organizations that criminal threats are targeting US financial institutions, capital markets exchanges, clearing houses, payment processors, businesses and consumers.

I want to thank you for the opportunity to address the issue of corporate account takeover. Corporate account takeover is the unauthorized use of valid online banking credentials, typically obtained via malicious software ("malware") that infect customers' workstations, laptops or computer networks. Cyber criminals use a variety of methods to infect business customers' computers and they are constantly updating their methods to match customers' uses of technology.

In order to get account information, cyber criminals continue to attack business customers' computers by phishing (attempting to acquire information (and sometimes, indirectly, money) such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication), malicious advertisements (or "malvertisements") and fraudulent messages on social media sites.

Phishing remains the most popular attack method that criminals use to infect victims' machines. Nonetheless, emails that purport to be from a victim's bank are no longer the primary type of phishing email. Criminals now send emails purporting to be from NACHA (The National Automated Clearing House Association), EFTPS (the Electronic Federal Tax Payment System), the US Postal Service, private delivery firms, telecommunications' companies, social media providers and others in order to trick their victims into opening the email and clicking on a link. Once the user clicks on such a link, it redirects the unknowing user to a server that then downloads malicious software onto the victim's computer. This malicious software includes a key logger (a program that can record a user's keystrokes) that captures the user's online banking credentials as he types them.

Another method of attack is malicious advertisements or "malvertising." In this case, criminals have put advertisements on search engines and other prominent news-sites. Victims, believing that it is a legitimate ad, click on the link, and the malware gets downloaded on their computer(s) and fraud can occur. A more recent method involves fraudulent messages sent from social media sites. These may include bogus friend requests, for example, that include links to malicious sites.

Once the criminals have the valid online banking credentials, they can impersonate the customer by logging onto the online banking site. They then create fraudulent ACH and/or wire transactions which they submit to the bank. The fraudulent transactions are generally directed to people who have been recruited to serve as intermediaries or "mules." The mules receive instructions from the criminals regarding how to handle the funds. The mules might be instructed to withdraw the funds in cash and then send them elsewhere via legitimate money transfer or wire methods. The mules get to keep a percentage of the funds as payment for his/her services.

However, research shows that losses due to cyber crime currently only account for a small percentage of the overall fraud losses incurred by financial institutions. Over the past two years, actual losses experienced by financial institutions and their customers as a result of cyber-related fraud has actually declined in spite of the fact that the number of attacks has increased. The FS-ISAC and its members recognize the online criminal threat both to the affected institutions and to consumer confidence posed by these criminal activities and we are taking steps to address areas of concern.

The FS-ISAC has been active in its efforts to counteract the spread of corporate account takeover. In 2010, the FS-ISAC formed the Account Takeover Task Force (ATOTF) as a result of continued concern and need for additional tools to help financial institutions and their customers combat online account takeover attacks. The ATOTF consists of over 120 individuals from thirty-five financial services firms of all sizes and types, ten industry associations and processors and representatives from seven government agencies. The ATOTF recently completed a report that includes recommendations to focus on three main areas—prevention, detection and responsiveness—in order to ensure an improved and effective defense against cyber crimes, including account takeover.

For each area, the ATOTF created work products whose purposes were to assist financial institutions of all sizes with dealing with account takeover by educating them and their customers on how account takeover works, what techniques can be used to detect and prevent account takeover, and lastly, in the event of an account takeover event, what steps financial institutions and customers should take to respond.

Examples of the work products include:

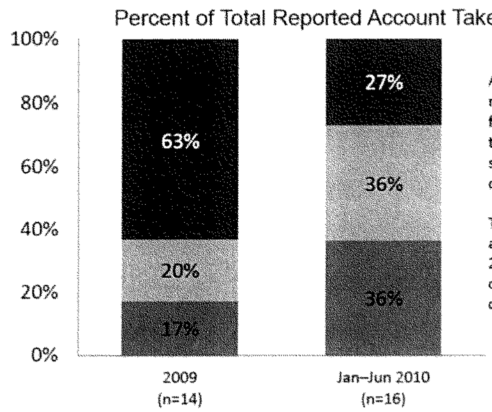
- Industry Advisories for Corporate & Small Business Customers and Financial Institutions
    - Fraud Advisory for Businesses: Corporate Account Take Over, co-branded with US Secret Service, FBI and Internet Crime Complaint Center (IC3) The advisory is available here: http://www.fsisac.com/files/public/db/p265.pdf
- J1-visa Mule Advisory (many mules from abroad are recruited via J1-Visas)
- Fraud Advisory for consumers about Work from Home Scams (where mules are often recruited)
    - Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams, co-branded with FBI and IC3. The advisory is available here: http://www.fsisac.com/files/public/db/p264.pdf
- Detailed white papers on Detection, Prevention and Response Techniques
- A contact list and procedures which provide financial institutions with the information they need to report account takeover attacks to the Secret Service, FBI, and other law enforcement agencies

- A recommendation to FINCEN (since adopted) to redesign the Suspicious Activity Report (SAR) in order to appropriately capture account takeover events

Lastly, the ATOTF has undertaken, with the assistance of the FS-ISAC and the American Bankers Association, surveys of the FS-ISAC members about the scope and impact of the account takeover problem. Survey data has been obtained for 2009, 2010 and the first half of 2011. The chart which follows includes a portion of the survey data for 2009 and 2010. This chart reflects the collective work of the ATOTF and FS-ISAC members in working effectively to reduce monetary losses associated with account takeover.

Monetary Transactions (ACH or Wire Transactions) Associated with Commercial Account Takeovers

Based on valid responses from FIs that reported experiencing account takeovers in 2009 and/or Jan-June 2010.



About a third (36 percent) of the reported account takeovers in the first half of 2010 had monetary transactions created but were stopped before the funds left the FI, compared to 20 percent in 2009.

Twenty-seven percent of reported account takeovers in the first half of 2010 had monetary transactions created and funds sent out of the FI, compared to 63 percent in 2009.

- ▨ No monetary transactions were generated
- ▨ Monetary transactions were created but were stopped prior to the funds leaving the sending FI
- ■ Monetary transactions were created and funds were sent out of the FI

*This graph includes only those banks that provided valid responses for all three categories.

FS-ISAC GREEN : The contents of this alert may be shared with FS-ISAC members, partners, and other ISACs.

In the most recent survey, members were asked about the most effective step they had taken to reduce corporate account takeover. The answer may surprise you. It was not technology or legislation; rather, it was customer education. As trusted partners, financial institutions are in the best position to educate our customers about the vectors of attack for corporate account takeover and how customers can protect themselves. This is why customer education was such an integral part of each ATOTF deliverable.

As noted above, the FS-ISAC and its membership have taken tremendous steps to limit cyber crime and corporate account takeover. Nonetheless, it is important to note that corporate account takeover attempts cannot be stopped solely by the actions of financial institutions. Beyond financial firms, our customers and participants in the broader electronic ecosystem all have roles to play to improve security.

Banks, for instance, have no direct control over the end customers' computers, nor can banks control what emails bank customers open or what websites they visit prior to accessing their online banking system(s). Nonetheless, to increase the security of our customers' accounts, we must educate our customers on the risks and monitor for anomalous transactions. Banks must continue to detect fraudulent transactions and stop them. Customers have a role to play in learning about these threats and practicing safe internet habits. Customers can also reconcile their accounts daily and review their electronic transactions for accuracy.

Others have roles to play as well. Law enforcement can assist by seeking out and arresting the criminals behind these attacks. Internet Service Providers (ISPs) can monitor traffic on their network for much of this malicious software and alert their customers to these infections. (Collaboration is already underway with the government, ISPs, and others to reduce the number of servers and computers used to disseminate the malware and phishing emails that target financial institution customers.) ISPs and email service providers can create electronic security measures that "interrogate" phishing emails. If the senders don't authenticate the messages, they should be dumped into spam folders so they are less likely to fool users. Also, these companies can pursue civil actions to take down servers that send the phishing emails and malicious software. Finally, continued work on international legal and diplomatic levels is needed so that all countries recognize this type of cyber-crime and that there are some forms of sanctions for those countries that harbor the criminals who perpetuate the problem.

Another example of industry collaboration is the BITS / FSISAC Trusted Email Registry project, which is designed to strengthen the email delivery channel through better authentication and encryption.

Let me highlight one example of cooperation. Law enforcement and a number of government agencies have taken a lead role working with the FS-ISAC, its member organizations, payments processors, and the financial services sector as a whole to combat these types of attacks. An example of a successful instance of government/financial services sector information sharing occurred on August 24, 2009, when the FBI, FS-ISAC and NACHA released a joint bulletin concerning account takeover activities targeting business and corporate customers. The bulletin described the methods and tools employed in recent fraud activities perpetrated against small to medium-size businesses that had been reported to the FBI. The objective of the bulletin was to employ FS-ISAC and NACHA subject matter expertise and apply it to the FBI case information to identify detailed threat detection, prevention, and risk mitigation strategies for financial institutions and their business customers, while preserving the integrity of the FBI's ongoing investigations. The FS-ISAC and NACHA developed a comprehensive list of recommendations for financial institutions to educate their business customers on the need to use online banking services in a secure manner. The bulletin was distributed through the FS-ISAC to its over 4,400 members, which includes over 30 member associations such as NACHA, ABA, and ICBA. Subsequent releases of the bulletin were shared with the press in 2010, redacting sensitive information about the ongoing investigations.

The risk mitigation tactics that are outlined in the joint FBI/FS-ISAC/NACHA bulletin include information security best practices that are consistent with the 2005 Federal Financial Institutions Examination Council's (FFIEC's) Guidance on Authentication in an Internet Banking Environment. The joint FBI/FS-ISAC/NACHA bulletin actually moved further than the 2005 FFIEC Guidance in its recommendations. Specifically, the bulletin recommended that financial institutions implement a layered "defense in-depth" approach to information security to protect financial institutions and their customers.

FFIEC SUPPLEMENTAL GUIDANCE ON INTERNET BANKING AUTHENTICATION

The FFIEC Supplemental Guidance on Internet Banking Authentication released on June 28, 2011 incorporates many "defense in-depth" recommendations and includes a number of very important new regulatory provisions that fit into the larger and detailed regulatory landscape. To highlight, the financial services sector is highly regulated by international, Federal and state authorities. Through numerous laws enacted by Congress over the past 150 years, federal financial regulators have implemented a complex regime that includes supervision of the financial institutions' operational, financial and technological systems. Regulators, such as the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency and Securities and Exchange Commission, conduct examinations to assess the adequacy of controls to address financial and other risks. These examinations focus on information security, business continuity, vendor management and other operational risks. In addition to these public sector entities, self-regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), the National Futures Association (NFA), and exchanges, such as the Chicago Mercantile Exchange (CME), and the New York Stock Exchange (NYSE), also play an important role in industry oversight.

The following is a summary of some of the Supplemental Guidance's key provisions. The Guidance reinforces existing supervisory expectations for annual risk assessments by financial institutions. These risk assessments should consider changes in the internal/external threat environment, changes in the financial institution's customer base, changes in functionality to online Internet services, and the financial institution's actual fraud experiences. Authentication controls should be upgraded in response to risk assessments.

For the first time, the FFIEC distinguishes between retail and commercial accounts. It raises the bar for minimum controls for all accounts and recognizes that commercial accounts pose a higher level of risk. The Guidance notes that banks must educate their customers on both the security and protections provided to both retail and commercial clients. In doing so, it creates a regimen of clear disclosures. Commercial account controls should be consistent with increased levels of risk and stronger than the controls for consumer accounts.

The FFIEC Supplemental Guidance now requires financial institutions to have layered security for consumer accounts. "Layered security" is defined as having different controls at different points in a process, so that weakness in one control is compensated by strength in another control. At a minimum, layered security should include anomaly detection and response at initial customer login, and at initiation of funds transfers to other parties. Layered security for commercial accounts should be stronger than those implemented for consumer accounts. The Guidance specifies enhanced controls for system administrators of commercial accounts. Examples of these enhanced controls include additional authentication/verification of new payees, creation of new wire templates, added wire approvers, and changes to established value threshold or time windows.

Layered security should now include anomaly detection. Changes in consumer or commercial account activity should be detected and steps taken (such as triggering incremental client authentication to validate questionable transactions) to ensure that additional controls are in place if such activity is discovered. Such efforts must protect customers' privacy yet should not interfere with efforts to detect fraud. However, according to the FFIEC Supplemental Guidance, "simple" device identification and challenge questions are no longer deemed effective as a primary control. Instead, financial institutions will be required to implement "*Complex Device*

Identification." An example of complex device ID includes use of a one-time cookie, in conjunction with other factors, such as the PC's configuration, IP address, and geo-location, to create a digital "fingerprint" of the customer's personal computer. The Guidance also calls for more "*Complex Challenge Questions"* not easily found by cyber criminals on the Internet. These "out of wallet" questions should not rely on publicly available information and there should be more than one question, potentially even including a "red herring" question that only the account holder will recognize as false, requiring a potentially fabricated answer.

Lastly, the FFIEC Supplemental Guidance calls for increased customer awareness/education efforts by financial institutions. The Guidance recognizes that customers have an important role to play in online banking security, and that consumers' and small businesses' financial institutions are likely more knowledgeable about online security. Financial institutions have an obligation to help customers practice good online banking security and to clarify, via customer education, the protections provided under Regulation E. Financial institutions should also educate their commercial account holders, especially small businesses, on use of security controls that are available for their online banking services.

FFIEC regulatory agencies have begun examinations to assess conformance with these new FFIEC Supplemental Guidance.

As a result of the 2009 joint FBI/FS-ISAC/NACHA bulletin, the FFIEC Supplemental Guidance and the many deliverables of the ATOTF, financial services firms and their business customers, government, and consumer customers have become more aware of the online risks facing them and of the many effective layered defense practices to mitigate those risks. As a result, more financial institutions are now aware of how to detect, prevent and respond to malicious and criminal activities resulting from online attacks.

FS-ISAC believes that the private sector and government can continue to work together to improve account security. Several areas of cooperation are outlined below.

1. IMPROVE CYBER CRIME LAW ENFORCEMENT
    a. There needs to be better and more domestic and international collaboration regarding investigations and prosecutions given the origins of a significant portion of cyber crime. Countries that have not adopted the Council of Europe's Convention on Cyber Crime should be encouraged to do so. The Convention is an international, multilateral treaty specifically addressing the need for cooperation in the investigation and prosecution of computer network crimes.
    b. Sufficient funding is needed for cyber crime investigations and forensics. Currently, private sector firms report that some local law enforcement agencies require minimum thresholds before they will take the case. However, evidence indicates that most of these types of attacks are directed at many firms and their customers, so the cumulative dollar value of the crime committed may be many times the amount of any individual loss.
    c. Law enforcement must be more responsive to cyber crimes reported by financial services firms. There needs to be improved communications at a local level between financial

services firms and their cyber crime law enforcement contacts and an understanding of how to report these crimes so that action will be taken.

d. After a compromise is reported to law enforcement, law enforcement must allow the threat indicators from the attack to be shared with financial institutions. There are a number of instance where those indicators have not been shared and thus other financial institutions are exposed to similar attacks. We understand the sensitivity around nation state attacks and around preserving evidence for criminal cases. However, the actions of some law enforcement agencies to restrict information sharing is hampering the financial services' sector's ability to protect itself and its customers from similar attacks. This issue speaks clearly for the need for greater trust between the public and private sector.

e. In keeping with our commitment to education, it is also important for law enforcement, prosecutors and judges to have substantial cyber education and knowledge so that they can prosecute cyber criminals effectively.

2. CONTINUE TO IMPROVE FINANCIAL INSTITUTION INFORMATION SECURITY PROGRAMS

Regulators and industry need to have a flexible and dynamic approach to cyber security so that individual financial institutions can continue to improve information security programs based on their size, scope of activities, and structure. Financial institutions have comprehensive security regulations already in place. This approach builds on the foundation embodied in the Gramm-Leach-Bliley Act framework and opposes prescriptive, one-size-fits-all or technology-specific approaches.

3. IMPLEMENTATION OF DEFENSE IN-DEPTH SECURITY

Financial services firms and payment processors need to implement defense in-depth security in order to protect their customers and their institutions from cyber criminal attacks. These security solutions must take into account the evolution of the changing threat landscape and will need to be updated over time. Commercially reasonable security procedures must achieve an appropriate balance between security, risk and usability. The June 28, 2011 FFIEC Supplemental Guidance on Internet Banking Authentication goes a long way towards achieving that balance without dictating any single solution which may prove to be untenable over time.

4. IMPROVE PUBLIC/PRIVATE SECTOR COLLABORATION

Expanded information sharing between government agencies and the financial services industry is one of the FS-ISAC's primary goals. There have been improvements made but there needs to be greater private sector access to threat and intelligence from Federal intelligence and law enforcement agencies. The House-backed Cyber Intelligence Sharing and Protection Act is a good example of strengthening information sharing in order ultimately to protect customers. This access must be administered in a manner that can provide broader protection without providing undue market advantage to a select group or that would compromise ongoing investigations. Specific recommendations include:

a. Provide financial institutions, networks and processors with timely, relevant and actionable information on threats, vulnerabilities, and exploits.
b. Provide the financial services industry with analysis of trends using existing data reporting requirements (e.g., FinCEN's data of Suspicious Activity Reports which includes computer crimes).

c. Support the existing National Infrastructure Protection Plan (NIPP) and its supporting organizations such as the National Council of ISACs of which the FS-ISAC belongs and the sector coordinating councils, such as the FSSCC. Also support the FSSCC's public sector partner, the Financial and Banking Information Infrastructure Committee (FBIIC) and support their joint initiatives.

d. Compile and share data on payment system fraud and security trends.

e. Fund top R&D priorities, such as the FSSCC's priority project on identity assurance.

f. Support industry exercises that relate to cyber threats. By routinely engaging in exercises and training, public and private sector participants build relationships and establish trust that is essential for sharing information.

g. Continue towards the goal of a fully integrated Joint Coordination Center for sharing cyber threat information between the public and private sectors. The embedding of financial sector personnel in the NCCIC is a positive step in that engagement process and is an essential building block towards a stronger trust model.

5. IMPROVE THE INTERNET INFRASTRUCTURE

Use Federal procurement power to improve the security of software, hardware and services that support the Internet business infrastructure and applications (i.e., enhanced technology that is implementable and cost appropriate for the market.)

6. EDUCATION

More public/private sector collaboration is needed to support educational efforts to increase consumer and business awareness of cyber threats and risk mitigation best practices. One example of such an effort has been undertaken by the National Cyber Security Alliance in promoting a "Stay Safe Online" campaign as part of the October Cyber Security Awareness month (http://www.staysafeonline.org/).

As a result of these types of programs and the efforts of the FS-ISAC Account Takeover Task Force, financial institutions have educated their customers regarding phishing and other social engineering attacks with information on their websites, mailers and in their bank lobbies regarding safe and secure online banking practices. Corporate and government users of online financial services products can now take advantage of these educational tools that are available.

Thank you for the opportunity to present this testimony.

House Committee on Financial Services
Subcommittee on Capital Markets and Government Sponsored Enterprises

Hearing on "Cyber Threats to Capital Markets and Corporate Accounts"

Mark G. Clancy
Managing Director and Corporate Information Security Officer
The Depository Trust & Clearing Corporation

June 1, 2012

Chairman Garrett and Ranking Member Waters,

Thank you for scheduling today's hearing on the important issue of cyber security and the U.S. capital markets. The Committee's strong leadership on this issue has been critical in helping to raise awareness of the serious threats posed by cyber-attacks on the financial system and fostering dialogue among the private and public sectors on effective strategies to minimize these risks.

My name is Mark Clancy, and I am the Corporate Information Security Officer at The Depository Trust & Clearing Corporation ("DTCC"). DTCC is a participant-owned and governed cooperative that serves as the critical infrastructure for the U.S. capital markets as well as financial markets globally. Through its subsidiaries and affiliates, DTCC provides clearing, settlement and information services for virtually all U.S. transactions in equities, corporate and municipal bonds, U.S. government securities and mortgage-backed securities and money market instruments, mutual funds and annuities. DTCC also provides services for a significant portion of the global over-the-counter ("OTC") derivatives market.

To provide insight into the criticality of DTCC's role in the safe and efficient operation of the U.S. capital markets, in 2010, the Depository Trust Company ("DTC") settled more than $1.66 quadrillion in securities transactions. Furthermore, three DTCC subsidiaries last month received notifications from the Financial Stability Oversight Council ("FSOC") of proposed determinations to designate them as systemically important financial market utilities. The subsidiaries are National Securities Clearing Corporation ("NSCC"), the clearing and settlement subsidiary for equities and corporate and municipal fixed income securities, Fixed Income Clearing Corporation ("FICC"), the clearing and settlement subsidiary for U.S. Treasury, Agency and Government-Sponsored Enterprise mortgage-backed securities, and DTC, the depository subsidiary. DTCC itself, as the parent and holding company of these subsidiaries, did not receive a letter, and it does not expect one. As the primary infrastructure responsible for the clearance and settlement of nearly all securities traded in the US cash markets, these DTCC subsidiaries play critical roles in mitigating risk and ensuring the safe and seamless operation of the U.S. capital markets.

I am going to focus my testimony today on providing an overview of DTCC's approach to managing the cyber risk environment. Then I will highlight the nature of the cyber-threats DTCC faces as an organization, how DTCC and the industry plan for and respond to these potential attacks on the infrastructure and opportunities for the private sector and government to work collaboratively to enhance cooperation and information-sharing to protect the safety and soundness of the capital markets.

Understanding the Risk Environment

Due to DTCC's unique role standing at the center of the financial services industry, the organization brings a dual perspective to its view of the risk environment. First, DTCC must examine and plan for cyber-attacks that could impact its ability to perform clearance and settlement and other critical post-trade processes that underpin the global financial marketplace. While these operational risks have long defined the risk landscape for DTCC, in recent years the organization has expanded its focal point to also include liquidity and market risks related to cyber-threats. Second, because of the interconnectedness of the financial system, DTCC must also take into account the broader systemic risks that could result from a cyber-attack on its systems.

To understand the nature and extent of the threats faced by DTCC, the organization regularly conducts enterprise-wide risk assessments, including a thorough analysis of business functions and the facilities, systems, applications, business processes and people that perform them. Next vulnerabilities that might exist within those assets and the controls in place to mitigate them are examined. Finally, the threats that exist to those assets are analyzed. The combinations of those factors determine the level of residual risk in the organization – that is, the risk that remains despite efforts at mitigating it.

Armed with this data, DTCC assesses whether the residual risk is above, below or consistent with the level of risk that DTCC considers acceptable (known as risk tolerance). This data informs the organization's business planning and helps guide decision-making on the need for additional investments to further reduce risk or a readjustment of risk tolerance. As these questions are considered, DTCC must also weigh the cost of achieving a tighter risk tolerance against the risk of not acting at all.

Risk assessment is a dynamic process, but certain aspects of it are more dynamic than others – and the area that is most volatile are changes in threats and vulnerabilities. On a practical level, virtually no organization has the capability to reduce threats on a daily basis. Rather, organizations must focus their efforts on mitigation of vulnerabilities and/or strengthening of controls. Vulnerabilities take many forms, and while some can be addressed relatively quickly and easily, others require complex and lengthy solutions. DTCC has numerous systems and processes in place to identify new vulnerabilities that could threaten the infrastructure, but the reality is that the organization does not control the timing of their discovery. Indeed, the only variable DTCC, or for that matter, any corporation, fundamentally controls is the tempo at which those vulnerabilities are mitigated. Through continuous analysis and review, DTCC makes decisions on investment levels in response to this rapidly-changing risk environment.

The Systemic Impact of Cyber Attacks on DTCC

The global financial system is an enormous, interconnected "system of systems." In other words, while individual institutions operate different parts of the critical infrastructure, the financial system itself is a product of the interactions of all these discrete actions. Because DTCC is connected to thousands of different market participants spanning the entire financial services industry globally, the organization must look beyond how a cyber-attack could harm its own operations to the systemic impact on its members and the broader financial community.

As mentioned earlier, DTCC serves as the critical infrastructure for global financial markets and, in this capacity, DTCC acts as an integration point that connects a wide range of industry participants. If DTCC is unable to complete clearance and settlement due to systems disruptions or outages, buyers and sellers of securities would not know if their trades had completed and, therefore, what securities they own or how much capital they have.

DTCC's financial risk and operational assessments must take into account these essential functions and determine how non-performance would impact the markets it serves as well as the firms that utilize its products and services, the investing public and the U.S. economy. In other words, if a cyber-attack directed at DTCC rendered its systems non-operational, what would that do to the overall functioning of the financial system? If the financial markets could not operate, how would that affect liquidity and access to capital? This systemic view of cyber risk has driven DTCC to broaden its perspective to include consideration of ways to mitigate low frequency but potentially high-impact scenarios that a monoplane risk assessment would have ignored.

Threat Actors: Criminals, Hackivists, Espionage and War (CHEW)

It is easy to overgeneralize the threat actors who engage in cyber-crimes as identity thieves who infiltrate computer systems to steal personal data or cyber terrorists who want to declare "war" on a particular nation or the world by disrupting the efficient operation of the financial system. Richard Clarke, the counter-terrorism expert who worked as an adviser to Presidents George W. Bush and Bill Clinton, developed a simple way to classify the different "threat actors" into four distinct categories – Crime, Hacktivism, Espionage and War (CHEW). In some cases, I have modified Clarke's definitions to reflect my own views on and experiences with these subjects.

Crime

The motivation of this group is financial gain and, according to the U.S. Treasury, they have been successful. A study by the agency found that cyber-crime accounts for more revenue than international cartel drug income, running into the hundreds of billions of dollars annually. The threat intensity of this group varies based on two factors: the capabilities of the actors and the vulnerabilities of the targets. While organizations are continually assessing and addressing potential weak links in their systems, criminals are just as quickly acquiring new technical skills and capabilities through a sophisticated cyber black market.

Hacktivism

The term hacktivism is applied to groups or individuals who use computer intrusion or "hacking" techniques to promote and publicize an often radical political point of view. The most prominent example of hacktivism is the group Anonymous, which supports efforts of the website WikiLeaks to publish private, confidential information of governments and corporations to expose what it believes are injustices or other perceived wrongs. When members of the U.S. financial sector stopped accepting payment transactions for merchant accounts from WikiLeaks, Anonymous lashed out by initiating denial of service attacks (attacks designed to make a system or network unavailable for use) against a number of those financial firms, including MasterCard, Visa and PayPal. This group, like virtually all hacktivists, is not motivated by financial gain – it wants to make a high-profile political statement. The capabilities hacktivists vary greatly, although it is common to find a few highly-skilled individuals operating in loose confederation with lesser-skilled but highly-motivated actors. The attacks from hacktivists are more difficult to predict because their target selection is often done by consensus online and sometimes in real time.

Espionage
The term cyber espionage was coined to reflect the "spy vs. spy" activity that has occurred between nations for millennia. However, cyber espionage has expanded in recent years beyond attempts to steal national secrets to now include cyber theft of proprietary information from corporations in an effort to gain an economic and competitive advantage over the commercial interests of that country.

The U.S. Office of the National Counterintelligence Executive released a report to Congress in 2011 highlighting the nature of the problem. [1]

> "In 2010, the FBI prosecuted more Chinese espionage cases than at any time in our nation's history. Although cyber intrusions linked to China have received considerable media attention, some of the most damaging transfers of U.S. technologies to foreign entities have been conducted by insiders. For example, a DuPont chemist in October 2010 pled guilty to stealing research from the company on organic light-emitting diodes, which the chemist intended to commercialize in China with financial help from the Chinese Government.
>
> Similarly, the unmasking of the network of 10 Russian "illegals" implanted on American soil indicated that these spies had been tasked to collect on economic as well as political and military issues.
>
> China and Russia are not the only perpetrators of espionage against sensitive US economic information and technology. Some US allies abuse the access they have been granted to try to clandestinely collect critical information that they can use for their own economic or political advantage." [2]

War
This is the cyber age equivalent of Carl von Clausewitz's 19th century definition that "war is the continuation of politics by other means." In this regard, war generally refers to the launch of a cyber-missile or some other cyber weapon of mass destruction to devastate the capabilities of a government or corporation by causing a physical system to fail or to gain control over that system. Today, as many as 30 countries have cyber war units to protect and defend against such

---

[1] http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
[2] http://www.ncix.gov/issues/economic/index.php

an attack, according to Secretary of Defense Leon Panetta, who also oversees a cyber-command center comprised of Army, Navy, and Air Force personnel.

There is another aspect of war thinking that attempts to undermine the integrity of and reduce confidence in the capabilities of a particular technology system(s) to the point that it is rendered too unreliable or error prone to be used for mission critical functions. An example would be cyber criminals tampering with the system(s) of an electronic exchange to the extent that investors lacked confidence in its ability to provide accurate prices or efficient matching of buyers and sellers.

Cyber Threats to the Capital Markets

The universe of threat actors, regardless of which category they fall into, pose a significant and growing number of dangers to the U.S. capital markets, ranging from the theft of confidential data to preventing the critical infrastructure from performing key market functions to damaging the integrity of market data and information. Let's look at each of those in more detail.

Loss of Confidentiality of Data

The loss of confidentiality of personally-identifiable information, whether the result of neglect by employees of a firm or by malicious acts of external individuals, has the potential to put the investing public in harm's way for fraud and identity theft. If the frequency of these cyber-crimes occurs are regular, it could erode investor confidence in the capital markets.

The theft of a customer's access credentials when stolen via malicious software installed on the individual's computer is particularly dangerous because that customer faces the potential loss of his or her funds. When this type of theft occurs on a grander scale involving thousands, tens of thousands or even millions of individual account holders, cyber criminals have the power to engage in market manipulation via "pump & dump" scams. In this example, the thieves can run up the price of a thinly-traded security they own by creating buy and sell orders in the accounts they have taken over. Their goal is to move the market in that stock by biding against themselves and anyone else they can lure into the scam.

More sophisticated criminal groups sometimes target high-value victims, including institutional clients and prime brokerage accounts, which tend to hold larger balances and normally transact with international locations, for the same purposes. The international nature of these crimes makes detection difficult.

Finally, DTCC has seen in recent years attacks using highly sophisticated social engineering techniques that target corporate deal-making information, particularly in the commodities and mergers and acquisition spaces. While this information cannot be easily converted into cash, the crimes are indicative of economic espionage and attempts to give foreign corporation or nations an advantage in competitive negotiations, such as those related to winning bids for natural resources or beating the offering price for an acquisition of a company.

Loss of Ability to Perform Market Functions

The National Market System (NMS) in the United States, which allows for the structured electronic transmission of securities transactions in real-time, is a prime target for threat actors who want to disrupt the orderly and efficient operation of the capital markets. While there are no public reports of the NMS being directly impacted by a cyber-attack that compromised the availability of key market services in the U.S., there have been instances of such crimes overseas. For example, in August 2011 the Hong Kong Stock Exchange [3] had to suspend trading in certain securities following a denial of service attack that made corporate filing information unavailable. As a result, the securities effectively became illiquid after trading was halted, which negatively impacted both individual and institutional investors in that market.

In 2012, hacktivist groups perpetrated a series of denial of service attacks directed against the public web sites of several U.S.-based stock exchanges. These attacks, while successful in blocking the availability of these online resources for brief periods of time, did not impact the operation of the NMS, but it reinforced the determination of hacktivists to shock the public and disrupt market activity.

If an attack on the NMS were to occur, particularly one that targets critical market infrastructure(s), it could pose serious consequences for the U.S. capital markets and the broader U.S. economy. The systems in the U.S. that perform these core processing functions are largely attached to private, interconnected networks. Although the Internet is not a core component of the NMS, it is commonly used to connect market participants to various systems as a back-up to dedicated telecommunications lines or as a direct connection for smaller market participants. While this minimizes the likelihood of such an attack, mainly because it would need to be conducted from inside the infrastructure or the private networks of market participants, the issue is serious enough that it remains a primary area of concern for the financial services industry.

Loss of Integrity of Information

Maintaining the integrity of financial data is a top priority of the industry because most financial assets in today's capital markets exist overwhelmingly in digital form. The transition from a paper-based environment to an electronic one was the result of a multi-year initiative to "dematerialize" securities or "immobilize" them in centralized depositories such as DTC. Today, for example, roughly 90% of the $36.5 trillion in securities held at DTC exist only in digital form. Similarly, at the beneficial ownership level, a significant percentage of broker/dealers have digital records detailing which retail and institutional customers own which securities while custodian banks maintain that information for other institutional clients, such as pensions and mutual funds. Financial firms take extreme precautions to guard against three main types of incidences that could impact the integrity of this data.

The first incidence is loss of integrity due to accident. The digital nature of the books and records of the financial system makes it critical that this information is secure. As a result, the industry has developed an elaborate set of check and balances when changes are made to these records to protect the accuracy of data and minimize occurrences of accidental errors.

The second incidence is loss of integrity due to malicious acts. In March 2011, for example, a service provider used by both the London Stock Exchange and Italian Borsa was hosting malicious banner ads[4] on the public web sites of these exchanges. While this was not a compromise of the exchanges trading systems, it represented vulnerabilities in the supplier processes for vetting paid advertisement content. The implication of this attack is that customers who normally interact with these exchanges could have been targeted in what would have otherwise appeared to have been a normal valid business request to the web site.

---

[3] http://www.bloomberg.com/news/2011-08-10/hong-kong-exchange-halts-some-trading-after-website-glitch-1-.html

Another example worth mentioning occurred in January 2011, when the European market for carbon credit trading [5]was temporarily shut down by cyber criminals who changed the ownership information of individual carbon credit owners. According to public reports, this scheme resulted in the theft of 30 million euros worth of credits from the Czech Republic, Austria, Greece, Estonia and Poland emissions market and the closure of the EU Emissions Trading System for more than a week.

The third incidence I'd like to mention is loss of integrity due to conflict between nations, terrorists and/or proxies. This type of cyber-crime involves threat actors infiltrating and maintaining access inside a system or systems of a government or corporation for the purposes of launching an attack at an undetermined point in the future. While it is somewhat difficult for a corporation to assess the likelihood of such an attack given the uncertainty in motivation of the threat actors, this has the potential to be the most catastrophic attack of the three I've mentioned today and the number of incidences has risen sharply in recent years. It is interesting to note that the more highly-skilled groups or individuals who could plan and execute such an attack tend to be more heavily invested in the orderly operation of the U.S. capital markets and, therefore unlikely to engage in this activity. However, those with less technical skills, most of whom are not as invested in the U.S. capital markets, are more likely to launch this type of attack and are working diligently to acquire the necessary capabilities.

DTCC's Approach to Protecting Against Cyber Threats

DTCC maintains an elaborate and sophisticated information security program to protect against the types of cyber-attacks mentioned above. While DTCC corporate policy calls for maintaining strict confidentiality of this information to prevent cyber criminals from knowing the full range of resources and capabilities we possess, we can share certain general information and protocols with the Committee as a way to provide insight into how DTCC safeguards its systems and the data we hold on behalf of customers and the financial services industry.

DTCC has established robust policies and procedures that provide the framework for information security within the organization. These policies cover both physical and logical security, are standards based (ISO 27001 and ISO 27002)[6] and are routinely refreshed to ensure the highest degree of protection against cyber-attack. DTCC's Information Security team carries out a series of processes, including preventative controls such as firewalls and appropriate encryption technology and authentication methods as well as vulnerability scanning to identify high risks, to protect the organization and its members in the cost-effective and comprehensive manner possible.

---

[4] http://www.techweekeurope.co.uk/news/london-stock-exchange-site-flagged-for-serving-malware-22376

[5] http://www.praguepost.com/news/7340-carbon-credit-thieves-still-at-large.html

[6] ISO/IEC 27001and ISO/IEC 27002 is an Information Security Management System (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The full name is ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems and ISO 27002 is Information technology - Security techniques - Code of practice for information security management. The two standards together formally specifies a management approach that is intended to bring information security under explicit management control and define 'best practice' recommendations for a control foundation for the protection confidentiality, integrity, and availability of information. These are global standards that are widely used across many industries. The two standards together

Public and Private Sector Collaboration Helps Protect Against Cyber Threats
The financial services industry is engaged in a variety of public-private partnerships with the federal government to protect against cyber threats and safeguard the nation's critical market infrastructure. A prime example of this collaborative relationship is the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). The FSSCC was established in 2002 in response to the September 11, 2001, terrorist attacks and at the request of the U.S. Treasury Department in harmony with Presidential Decision Directive 63 (PDD63) of 1998. PDD63 required sector-specific federal departments and agencies to identify, prioritize and protect United States critical infrastructure and key resources and to establish partnerships with the private sector.

The FSSCC has 52 member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government sponsored enterprises, investment banks, merchants, retail banks and electronic payment firms. FSSCC members dedicate a significant amount of time and resources to this partnership for critical infrastructure protection and homeland security. The FSSCC does not collect dues and its success as a volunteer organization relies heavily on the time members contribute and to the expertise and leadership roles members play within their respective financial institutions and associations.[7]

The FSSCC is charged with "strengthen[ing] the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the U. S. Federal government, and coordinating crisis response – for the benefit of the Financial Services sector (the "Sector"), consumers and the U.S.A."

The FSSCC has achieved a number of successes at overseeing cyber security efforts within the sector and has played a vital role in helping to identify strategic issues and coordinate a response with federal counterparts. One particular effort was the launch of a "threat and vulnerability matrix" to gather detailed information to perform an assessment at the sector-wide level, with the goal of identifying areas of common concern. In addition, the FSSCC has served as the coordinating entity in the private sector, working with the U.S. Department of Homeland Security (DHS), U.S. Treasury and other federal agencies, in getting cleared sector personal briefed at the classified level on contextual information about cyber and physical threats.

---

formally specifies a management approach that is intended to bring information security under explicit management control and define 'best practice' recommendations for a control foundation for the protection confidentiality, integrity, and availability of information. These are global standards that are widely used across many industries.

[7] http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Carlin_0.pdf

DTCC has been actively involved with FSSCC since its inception. From May 2004 to June 2006, DTCC's current President and Chief Executive Officer, Donald F. Donahue, served under an appointment by the U.S. Secretary of the Treasury as Sector Coordinator; he later served as Chair of FSSCC from April 2005 to April 2006. Currently, DTCC officials serve on various FSSCC committees, sub-committees and working groups, including the Executive Committee, Policy Committee and Sector Wide Activities Committee.

Financial Services–Information Sharing and Analysis Center and Information Sharing
The Financial Services–Information Sharing and Analysis Center (FS-ISAC) is the primary group for information sharing between the federal government and the financial sector. It was created in 1999 in response to the 1998 PDD63, which called for the public and private sector to work together to address cyber threats to the nation's critical infrastructures. After the terrorist attacks of 9/11, and in response to Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to include physical threats to the financial sector.

The FS-ISAC is a 501(c)6 non-profit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time, the membership has expanded to over 4,200 organizations, including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors and over 30 trade associations representing the majority of the U.S. financial services sector.

The FS-ISAC has implemented a number of programs in partnership with the Department of Homeland Security (DHS) and other government agencies to encourage and expand information sharing.

In 2011 , for example, the FS-ISAC, in partnership with DHS, became the third ISAC to participate in the National Cyber Security Communications Integration Center (NCCIC) watch floor. FS-ISAC representatives, cleared at the Top Secret/Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents and potential or known impacts to the financial services sector. This program has been extremely beneficial in providing situational awareness to the financial sector while also allowing the industry to provide feedback on threats to DHS.

DTCC was a founding member of the FS-ISAC in 1999 and continues to participate in the group's information-sharing mission. I currently serve on the Board of Directors for the FS-ISAC and as a member of the Threat Intelligence Committee (TIC). Team members are also active in the TIC, the Security Automation Working Group, Products & Services Committee, Audit and Compliance Working Group, Clearing House and Exchange Forum (CHEF) and Crisis Management team.

FSSCC & FS-ISAC: A Partnership to Combat Cyber-Threats
While the FSSCC operates at a strategy and policy level, the FS-ISAC engages with its members on operational issues. Together, the two bodies work in partnership to bring a more

comprehensive approach to cyber security. For example, the FSSCC and the FS-ISAC have been successful in partnering with DHS and the United States Treasury to obtain security clearances for over 250 individuals in the financial sector who support critical infrastructure protection.

The FS-ISAC serves as the hub of activity to coordinate information sharing on threats between financial institutions and the federal government, law enforcement and other critical infrastructure organizations. A sub-community within the FS-ISAC, CHEF was established in 2011. This sub-group played a critical role coordinating information sharing in response to a series of denial of service attacks on the public websites of U.S. stock exchanges. CHEF pooled intelligence, aggregated information about the characteristics of the attacks and shared strategies and techniques to mitigate them in near real-time. This information was shared with CHEF members and, more broadly, within the FS-ISAC and by the FS-ISAC with other ISACs, law enforcement and DHS. In addition, FS-ISAC members provided the CHEF with information about their approaches to mitigating attacks of this kind, which traditionally have not centered on the capital markets infrastructure. The key to success in managing these denial of service attacks was the level of trust that accompanied the information sharing between financial institutions themselves and these institutions and the federal government.

The FS-ISAC provides a host of additional resources for its members, including access to a library of threat information and alerts on new cyber threats and attacks. This enables the industry to more effectively monitor its own systems to determine if similar activity is occurring in their networks or to better align defenses to counter an attack before it occurs. Using the internationally recognized traffic light protocol (TLP), the FS-ISAC designates the sensitivity of unclassified information as green (can be shared with the widest audience), yellow (a somewhat narrower audience) and red (the most restricted audience) to ensure the widest but also most secure distribution of data.

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT)

There are two programs I'd like to highlight today because they are excellent examples of the enormous benefits that can be derived through a collaborative approach to information sharing between the federal government and the financial sector.

The United States Computer Emergency Readiness Team (US-CERT) leads the federal government's efforts to "improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks…while protecting the constitutional rights of Americans." [8] The US-CERT, using the traffic light protocol, provides alerts to the financial sector on observable data and indicator information, including tactics, techniques or procedures used by cyber criminals or details about the threat actors. The two most effective reports the industry receives are the Cyber Information Sharing and Collaboration Program (CISCP) alerts, which combine a range of sources and provide normalized post-analysis reporting on threat intelligence, and the Early Warning and Indicator Notice (EWIN), which provides less refined but timelier information.

---

[8] (http://www.us-cert.gov/about-us/)

The quality and quantity of information the financial sector receives from DHS's National Cyber Security Division (NCSD) and US-CERT has been greatly improved in the last three years and has been essential in helping to protect the nation's critical infrastructure at a time of increased threats.

The financial services sector also has the ability to leverage other federal capabilities provided by DHS and/or National Institute of Standards and Technology (NIST), including the National Vulnerability Database [9](NVD), which holds information on over 50,000 software vulnerabilities in commercial and open source software products.

Additionally, the financial sector has increasingly adopted use of the NIST Security Content Automation Protocol (SCAP) [10]suite, which includes the Common Platform Enumeration (CPE)[11] to identify types of systems and software in use and the Open Vulnerability Assertion Language (OVAL)[12] to describe the technical characteristics of a system to determine if a specific software vulnerability is present. DTCC employs SCAP to automate internal processes for the identification and eradication of known vulnerabilities within its IT infrastructure. This offers the organization a cost effective and proven way to efficiently manage vulnerabilities.

To further enhance information sharing, DTCC and FS-ISAC are collaborating with DHS and other groups to develop a protocol to automate the machine-to-machine sharing of threat reporting information to reduce inefficiencies and latency.

Opportunities to Enhance Public-Private Cyber Security Collaboration

In May 2010, FS-ISAC and federal agencies took an important step forward in partnering to counter suspected state-sponsored acts of cyber espionage by creating a pilot program, known as the Government Information Sharing Framework (GISF).[13] This pilot program allowed for the sharing of advanced threat and attack data between the federal government and about a dozen financial services firms that were deemed capable of protecting highly sensitive information. The program operated successfully from May 2010 through December 2011 and was expanded to include the sharing of classified technical and analytical data on threat identification and mitigation techniques.

Unfortunately, the program was effectively terminated by the Department of Defense (DoD) in December 2011 for reasons that were unclear to pilot participants. However, while information sharing was expected to continue through DHS, this, too, was ceased in December 2011, eliminating an important source of threat data and analysis for the financial sector. Since the termination of GISF, more than 5 organizations in the financial sector have experienced threat activity from actors first identified to the industry through GISF reporting. Furthermore, an assessment by FS-ISAC indicates that these threats will continue to increase in the years ahead.

---

[9] http://nvd.nist.gov

[10] http://scap.nist.gov

[11] http://cpe.mitre.org/index.html

[12] http://oval.mitre.org/

[13] FS-IASC executed an agreement with DHS and the Department of Defense (DoD), referred to within FS-ISAC as the Government Information Sharing Framework (GISF), based on an initiative with the Defense Industrial Base (DIB) companies, known as the Defense Collaboration and Information Sharing Environment (DCISE).

There were four primary benefits and insights that DTCC and the other pilot participants gained from GISF:

1. The receipt of actionable information in a format that allowed industry participants to search for similar threat activity in their own networks.

2. The receipt of contextual information on that actionable information to better understand the risk implications of observing that threat activity.

3. The ability to adjust assessments of cyber espionage using quantifiable information on the level of malicious activity being observed, which was previously invisible to members of the financial sector. This information greatly increased the collective assessment on threats that were present from these actors and resulted in the FS-ISAC substantially escalating its level of commitment and engagement with government and other partners to identify and mitigate these potential cyber-crimes.

4. An enhanced understanding that previous threat management processes, teams and tools had insufficient capacity to consume threat data due to its raw state and the level of inefficiencies in how this information was communicated. Today, the financial sector and DHS are actively collaborating on the development of standards to support the automation of sharing and consuming threat data.

GISF was responsible for driving innovative new programs in the industry to reshape the sector's approach to assessing the multitude of risks associated with cyber espionage. This prompted many of the pilot firms, including DTCC, to revise their views on best practices for managing threat information, to expand existing information sharing activities with peers and with the FS-ISAC and to make significant additional investments in threat mitigation and detection capabilities that otherwise could not have been easily justified due the lack of understanding of the risk to the sector.

Limitations of Classified Information to Protect Against Cyber-Threats

While DHS has been able to offer security clearance to more than 250 financial sector personnel for the purposes of giving them access to classified briefings, this is not sufficient on a practicable level because the data cannot be shared broadly due to its classified nature. Furthermore, the financial industry lacks the infrastructure and processing capabilities to handle such information, which typically provides additional context on non-financially motivated threat actors and their capabilities.

Next Steps: Expanding Information Sharing Between the Public and Private Sectors

Information sharing like that which occurred under the GISF program represents the most critical line of defense in managing and mitigating cyber security risk today because it:

- Provides actionable information for the industry to protect itself from cyber criminals;

- Drives innovation and improvement in defense strategies and programs, and
- Provides a vehicle for making risk-based decisions on investments and priorities.

While GISF was successful in many aspects, its reach and impact were limited because it did not scale to the depth and breadth of the sector. As a result, it is impossible to gauge the broader benefits of the program because only 16 financial institutions served as pilot participants. However, what is abundantly clear is that information sharing today occurs at "human" speed while cyber-threats occur at warp speed. Now more than ever, an investment in standards, protocols and methods for the industry to rapidly share and consume threat and observable data is needed.

In addition, information sharing is most valuable when there is a high degree of trust among and between the financial sector and federal agencies. The more trust that exists between these institutions, the more information sharing occurs – and the better equipped each organization is to mitigate the risk of cyber-attack and safeguard its systems and data from threats.

Also, there is a need for government to invest in additional staffing, tools and repositories to strengthen the nation's defenses against cyber-attack. Based on DTCC's experience and the increased need for collaboration between industry and government in this capacity, DTCC strongly supports restarting GISF, removing its pilot status and expanding its reach within the financial sector and to other members of the Critical Infrastructure and Key Resources (CIKR) community who face these types of threats. This program, in combination with supporting enhancement for standards and normalization (with an eye toward automation), will greatly improve the efficiency of threat detection.

A potential remedy that I'd like to share regarding the lack of classified processing capability within the financial industry is to enable the critical infrastructure community to engage service providers to provide the necessary capabilities. For example, telecommunications providers could filter the critical infrastructure firm's in-bound network circuits to remove threats in real-time based upon classified threat data that could not otherwise be processed at the firm. In addition, the federal government could allow the critical infrastructure firm to build and procure needed capabilities in their own infrastructure by allowing the accreditation of classified facilities to occur for non-government contractors.

Much of the depth of the U.S. government's understanding of cyber security threats is highly classified, and the CIKR community outside of the defense arena has limited personnel with the necessary security clearances. DHS has, at present, very limited ability to "hold" clearances for CIKR personnel. For example, recently-hired veterans at DTCC who held TS/SCI clearance from their military service saw those credentials lapse when they came to the private sector.

As the sophistication and technological means of threat actors increases, the financial sector and government need to move from a static one-size-fits-all framework to a risk-based one that incorporates the dynamic nature of the cyber security threat landscape, the individual firms in the financial sector and the global nature of the capital markets. Cyber-attacks on the financial services sector represent a significant risk not just to industry participants but to the stability and integrity of the global financial system itself. There are no shortage of threat actors who, for a variety of financial and political reasons, dedicate themselves to wreaking havoc on the systems that underpin the U.S. and global economies. While the public and private sectors have taken important steps forward in recent years to enhance collaboration, a greater degree of trust and information sharing is needed to ensure that all resources are working in concert to protect and defend the financial sector for cyber-attack. There is much progress to build on in the years ahead in these areas. DTCC stands ready to work in partnership with this Committee, the Congress and Administration and federal agencies to harden the sector's defenses against cyber-crimes.

On behalf of DTCC, I would like to thank you again for holding today's hearing to raise awareness of these issues and for allowing us to testify this morning. I would be happy to answer any questions you may have.

Testimony of Mark Graff
Vice President, NASDAQ OMX Group
Before the House Financial Services Committee
Subcommittee on Capital Markets

June 1, 2012

Thank you Chairman Garret, Ranking Member Waters and all members of the subcommittee. My name is Mark Graff. I am Vice President and Chief Information Security Officer in the Office of the Chief Information Officer at the NASDAQ OMX Group. On behalf of the NASDAQ OMX Group, I am pleased to testify on Cyber Security Issues.

Although I am new to OMX, having arrived in early April, I am no newcomer to information security, with about 25 years' experience in support of both industry and government. Most recently, I was head of cyber security at Lawrence Livermore National Laboratory, one of the crown jewels of research in this country and also a repository of many of this nation's most important secrets, such as nuclear weapon designs. I moved to NASDAQ OMX to help protect another part of America's critical infrastructure, its financial markets. I changed industries; but most of the challenges – and many of the adversaries – remain the same.

Although we are an integral part of the financial services community, NASDAQ OMX is as much of a technology company as many of the businesses that list on us. We own 24 markets, 3 clearing houses, and 5 central securities depositories, spanning six continents. Eighteen of our 24 markets trade equities. The other six trade options, derivatives, fixed income products, and commodities. Seventy exchanges in 50 countries utilize our trading technology to run their markets, and markets in 26 countries rely on our surveillance technology to protect investors and maintain a level playing field. We provide the technology behind 1 in 10 of the world's securities transactions.

NASDAQ OMX is committed to a vigorous defense of our infrastructure. NASDAQ OMX dedicates substantial capital and human resources, both internal and external, to ensure our systems are protected against a wide variety of attacks. As an expert in the methods used today to defend this nation's most highly classified networks from attack, I can tell you that we use many of the same technologies and techniques to defend NASDAQ OMX.

One key method at both institutions is the isolation of critical systems from the Internet at large. While many of the services we deliver to customers worldwide are housed on Internet-facing web servers, our trading and market systems are safely tucked away behind several layers of carefully arranged barriers, such as firewalls and network isolation zones. This is an important distinction to remember we should all keep in mind when hearing about "denial-of-service attacks" against one institution or another. Any troublemaker can run up to the front door of a house and ring the door bell over and over. That is what most "denial-of-service attacks" amount to. Sometimes, despite our best efforts, it may be difficult to reach one of our outward-facing websites for a few minutes as a result of such vandalism. When it happens, I ask you to remember that it does not mean, to return to my homely analogy, that anyone has broken into the house.

We do not rely on isolation alone. Our comprehensive information security program uses a multi-layered approach. NASDAQ OMX is continually looking ahead, identifying potential threats to the integrity of our systems such as information compromise, unauthorized system access, physical disruption, terrorist attacks, systems failures, and denial of service attacks. We then prepare for these threats through an ongoing program of information security protection and inspection, including the implementation of physical safeguards around data centers and work spaces; a consolidated network with multiple connectivity options; a disaster recovery plan for our infrastructure; capacity management and testing; and business continuity and crisis management plans.

In developing software, we treat information security as a critical element in the life cycles of our trading and corporate systems -- from initial planning, through deployment, and as part of ongoing operation.

In all of these areas, our information security program has strong senior management and board support, integrating security activities and controls throughout our business. These controls are complemented by extensive oversight by external auditors and the Securities and Exchange Commission. NASDAQ OMX continually evaluates and enhances processes to mitigate information security risks by implementing industry best practices as promulgated by organizations like the National Institute of Standards and Technology.

Below is a summary of the processes, policies and procedures that NASDAQ OMX generally follows in connection with information security:

- Business continuity plans are robust and take into consideration real time failovers of our market trading platforms, and protects against intentional or malicious attempts to disrupt our businesses.
- Information assurance at NASDAQ OMX addresses information security designed life cycle practices and controls necessary to secure our systems.
- NASDAQ OMX ensures that information is protected against unauthorized access and use by the following:
    - Traditional firewalls augmented with application layer protection.

- Host based security controls to protect against unauthorized modification and changes to the operating systems and extensive vulnerability and patch management programs to ensure the integrity of our infrastructure.

- Application security assessments, including source code review and penetration testing (by internal as well as third-party teams).

- Robust intrusion detection controls, continually updated and augmented, as part of a 24x7 monitoring process devoted to finding and mitigating cyber threats in real time.

- Assistance from third party corporations and individuals especially experienced in dealing with advanced threats.

These controls span our entire enterprise network. Our trading systems are further protected by their unique overall resilient architecture. Each trading platform, as I previously mentioned, is logically segmented from the corporate systems. It has a single point of entry and requires two-factor authentications for access and authorization.

In addition, the system restricts the information allowed to be submitted to it through the use of a fixed set of format protocols that not only controls inputs to the trading platform, but also restricts the scope and type of information that may be retrieved from the system. Finally, the trading platform is refreshed at the end of the trading day and no data is maintained in the trading platform beyond the trading day. During the trading day, NASDAQ OMX is capable of quickly observing and reacting to changes in normal data flows. Because the architecture of the system is set up to do one thing—accept and execute trade orders—activity that is not a trade order or an execution can be immediately observed and appropriate actions taken.

For all the steps that we take, NASDAQ OMX does have serious concerns about the worldwide attacks on critical infrastructure that are being led not just by rogue hackers, or organized crime, but are being backed by national governments. It is not reasonable to expect individual companies, no matter how large or sophisticated, to independently stave off cyber attacks coordinated and backed by a foreign government. If our headquarters or our physical infrastructure were under attack from foreign missiles the U.S. Government would work with us to defend our company. The same needs to be true for cyber attacks, especially since the U.S. Government is equally under attack from these foreign entities.

It is for this reason that we at NASDAQ OMX are very pleased that both houses of Congress are looking at ways to protect our critical national infrastructure through improved sharing of information about cyber threats and vulnerabilities. NASDAQ OMX supports the House passage of H.R. 3523, "Cyber Intelligence Sharing and Protection Act". Although there are concerns about data privacy that certainly need to be addressed, the bill has several good points that are necessary to curtail the numerous cybersecurity threats faced by business and government alike. Those points include:

- The ability for companies to obtain and share cyber threat information with any other entity including the federal government;
- Such shared information cannot be used by a cybersecurity provider to gain a competitive advantage;
- Such information when shared with the federal government cannot be used for regulatory purposes;
- No civil or criminal cause of action may be taken against a company acting in good faith that chooses not to act on such cyber threats obtained or shared in connection with the bill.

NASDAQ OMX is and will continue to be a willing partner with industry peers and government at every level, cooperating to protect the integrity of our critical infrastructure. Last October, for example, during Cyber Security month, NASDAQ OMX hosted Homeland Security Secretary Janet Napolitano along with a host of law enforcement agencies and financial services companies to discuss the importance of working together to address these issues. It will be my pleasure, as NASDAQ OMX's new CISO, to continue and expand such contacts and relationships.

Thank you again for inviting me to testify. I look forward to responding to your questions.

STATEMENT OF

BITS PRESIDENT PAUL SMOCER
ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

SUBCOMMITTEE ON CAPITAL MARKETS AND
GOVERNMENT SPONSORED ENTITIES
OF
THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON FINANCIAL SERVICES

CYBER THREATS TO CAPITAL MARKETS AND CORPORATE ACCOUNTS

JUNE 1, 2012

TESTIMONY OF PAUL SMOCER, BITS PRESIDENT

Thank you Chairman Garrett, Ranking Member Waters, and Members of the Committee for the opportunity to testify before you today.

My name is Paul Smocer and I am president of BITS, the technology policy division of The Financial Services Roundtable. BITS addresses issues at the intersection of financial services, technology and public policy, on behalf of its one hundred member institutions, their millions of customers, and all of the stakeholders in the U.S. financial system.

First, I would like to recognize the Members for their focus on cybersecurity as illustrated by the House's recent Cyber Week and, more importantly, by its passage of legislation that will enhance public/private information sharing, augment funding for cybersecurity research and development, and provide for broader citizen awareness and education regarding cybersecurity. These bills address three key issues in our collective effort to secure cyberspace and fight cybercrime.

The financial services industry recognizes the serious and constantly evolving nature of cyber threats to its customers, its institutions, and the broader economic wellbeing of the United States. The industry and its institutions have historically had and continue to have a strong focus on this subject and we have been leaders in partnering with others to address the challenges.

Today, I will address cybersecurity efforts at both the institutional and industry levels, collaborations within and beyond the industry, and efforts underway to improve information sharing, and discuss how both industry and government can be supportive in protecting key economic infrastructures, such as capital markets, and in protecting customers.

At the individual institution level, every new or developing product is subject to a risk assessment that the institution uses to identify potential institutional and customer threats and risks as well as to identify mitigations to limit these risks. Likewise, when institutions consider new product delivery channels, they too are subject to an in-depth risk review. The risk management practices and processes institutions use to conduct such reviews and their general efficacy is also the subject of reviews by numerous regulatory agencies that are part of the Federal Financial Institutions Examination Council.[1]

Individual institutions also bear a serious responsibility for understanding the cyber risks and controls of their key service providers. This is an important consideration as we consider cyber threats to both the capital markets and, to a more limited extent, commercial customers. In the context of capital markets, individual institutions often rely on external providers for many of the services that support this market such as clearings, settlements and accounting services. Institutions, both because of their innate risk management policies and regulatory expectations under the federal regulators' guidelines, regularly either examine the cyber and resiliency risks and controls of these providers or request the providers supply them with independently produced evaluations such as those produced under the American Institute of CPA's Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. These reviews both help assure that the underlying infrastructure that supports capital market security remains intact by forcing providers of services to employ effective cybersecurity protections and assures those using the services that they will remain available. Interestingly, many of the providers of those services are, in fact, themselves, financial institutions. As both a service provider and a financial institution, those institutions are both internally focused and externally focused on cyber issues.

Institutions recognize, however, that in the battle over cybersecurity, no one institution can fight alone. Consequently, at the sector level, a number of collaborative efforts exist. Through associations such as BITS and others such as the Financial Services – Information Sharing and Analysis Center (FS-ISAC) and the Securities Industry and Financial Markets Association (SIFMA) represented today on this panel, member companies band together to identify collectively institutional and customer risks in emerging areas such as mobile financial services, cloud computing and social media usage, as well as identify and share information on new threats and threat methods. They develop best practices guidelines for the industry to improve cybersecurity and reduce fraud. In many cases, these associations band together and work with all of their members on key issues. Two recent examples of these efforts include the work led by the FS-ISAC to address fraud occurring against commercial accounts through the Account Take Over Task Force and the work of the American Bankers Association and BITS toward building a more secure Internet environment in which to conduct financial services.

---

[1] See FFIEC IT Examination Handbook "Risk Management of E-Banking Activities" at http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities.aspx

The largest of these industry collaborations is perhaps the sector's Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). This group consists of over 20 financial trade associations, ten of the largest US-based financial institutions (many of whom are integral to providing services within the capital markets infrastructure) and ten key participants operating in the financial infrastructure such as the Depository Trust and Clearing Corporation (DTCC). Through the Council, these organizations come together to focus on key policy areas, threat and vulnerability, research and development and resiliency. One current focus of the group is a pilot program underway between the Council and the DHS Science and Technology Directorate's Cyber Security Division to utilize available government agency data to enhance customer identity verification – an effort that would be helpful in protecting consumers.

In the spirit of public-private partnerships, this Council works closely with the public sector partner Financial and Banking Information Infrastructure Committee (FBIIC), which was chartered under the President's Working Group on Financial Markets, and is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Chaired by the Treasury Department, this Committee includes sixteen government agencies with oversight for the entire financial sector including regulators within the capital markets. Working together, the Council and the Committee members focus on key cybersecurity issues affecting the industry and how to address them. This focus includes the critical question of the industry's ability to recover from an incident – whether cyber or physical – that might affect the availability of vital industry infrastructure. Under their leadership, the two groups have sponsored numerous industry-wide resiliency exercises. The latest of these, called "Quantum Dawn," had as one of its two objectives to exercise operational risk practices across the equities clearing and trading processes. The cybersecurity scenarios tested by this exercise included corruption of publicly reported stock prices, corruption of trades (changing of *buys* to *sells),* and substantial loss of availability of the National Market System and resulted in identifying both effective processes and areas for improvement.

While the industry and its regulators are investing significant effort to work symbiotically to improve cybersecurity for financial services, the effort continues even beyond those groups. Recognizing that our ability to maintain confidence in financial services relies on other key constituencies, the industry has formed collaborations with other key parties. One example is the development of the Cyber Operational Resiliency Review (CORR) currently being piloted. This pilot, organized by BITS, allows financial institutions to request, through The Department of the Treasury, a review by a team of specialists supplied by The Department of Homeland Security of an institution's cyber practices and networks. In addition, BITS, FS-ISAC and other associations have formed collaborative relationships with various law enforcement agencies including the Federal Bureau of Investigation, United States Secret Service and US Postal Inspectors to coordinate industry and law enforcement efforts to prevent and prosecute cybercrime. Law enforcement was a key participant in the efforts led by the FS-ISAC toward mitigating issues with commercial account takeover.

Understanding that it is important to strengthen every link in the infrastructure chain, the industry has also affected outreach efforts to other key sectors. One recent example was showcased this past Wednesday in a White House-sponsored event that announced the Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace developed by the Industry Botnet Group. This multi-industry group, committed to working together to combat cyber threats, is a voluntary group of corporations, trade associations, and non-profit organizations, led by a steering committee composed of BITS, Business Software Alliance, Online Trust Alliance, Software Information Industry Association, National Cyber Security Alliance / StaySafeOnline, StopBadWare, TechAmerica, U.S. Internet Service Provider Association, and the U.S. Telecommunications Association. Recognizing that botnets have a serious impact to the security and privacy of both individuals and businesses as they facilitate the delivery of malicious software by the cybercrime community, this multi-stakeholder group is acting collaboratively to mitigate the problem. Another recent example was the successful effort undertaken by Microsoft's Digital Crimes Unit – in collaboration with the FS-ISAC and NACHA – The Electronic Payments Association, to take down the command and control center of a major botnet ring operating within the US.

These types of efforts recognize a key factor – today's Internet and electronic world is highly integrated and relies on multiple organizations and providers to effectively mitigate security risks. That is why the industry has been and continues to be supportive of efforts to assure a more consistent level of security within other critical sectors in the cyber environment. That is also why the industry has invested in educating consumers on cybersecurity. Consumers and businesses play a key role in cybersecurity and have a responsibility to protect themselves as well. The financial services industry and others have recognized that consumers and businesses often lack the skills and awareness to fully protect themselves. As a result, significant investments have been made in education efforts by financial institutions and associations and we applaud the House's passage of H.R. 2096 The Cybersecurity Enhancement Act of 2012 sponsored by Representative Michael McCaul, which will help with this effort.

The industry's efforts start with individual institutions that provide educational materials via websites, mailings and community educational events. Financial associations also publish educational material and offer education directly to their communities through community outreach efforts. These efforts have often been done in collaboration with other parties such as law enforcement, as was the case with educating businesses about account takeovers, or with entities focused on citizen education such as the National Cyber Security Alliance and its StaySafeOnline campaign.

As these efforts show, the financial services industry understands cybersecurity is a critical issue, and that the best success in improving security comes from collaborative efforts and not just the work of financial institutions. Clearly financial institution work is significant in terms of resources, cost and commitment. Institutions willingly undertake these security and awareness efforts and recognize their necessity to safeguarding customers and their accounts, and the overall financial system. These protections are critical to maintaining customer trust and confidence in the industry, and are a highly important investment. Individual institutions also recognize success depends on investing in broader, collaborative efforts beyond financial services to ensure a resilient economic system.

I would be remiss, however, if I did not mention one other key area of collaboration – that is, the area of threat information sharing. Like all cybersecurity defenses, information sharing exists at multiple levels. Individual institutions monitor their own threats and in the financial services sector, we do an effective job of sharing threats through the FS-ISAC. But, there remains much opportunity to exchange threat information more broadly. Most of the efforts to date have involved intra-industry efforts in the financial services sector and in the defense industry sector, through its

Defense Cyber Information Sharing Environment (DCISE) program. Inter-industry and public/private information sharing opportunities remain to be developed. BITS, in cooperation with the FSSCC and the FS-ISAC, is nearing the end of a study to assess existing and potential collaboration programs between the US Government's national security agencies and the financial services sector. The study focuses on threat information sharing, cyber security capacity building and cyber-related crisis management.

Threat data and threat analysis are very often industry agnostic. Viruses, Trojans and other malicious software are sometimes written to attack the users of a particular sector, such as those that attempt to steal login credentials from banking customers. In many cases, however, they are not aimed at a particular sector. For example, malicious software that attempts to take over a user's computer or other device to make it part of a botnet[2] that will be subsequently used by cybercriminals simply does not care who or for what purpose one is using their device. Botnets, however, create the risk of establishing large numbers of endpoints available to criminals to commit cybercrime. Likewise, cyber anarchists who use denial of service attacks in attempts to disrupt the availability of systems, websites and other technology resources use these techniques to target entities in virtually all private and public sectors. The more information shared across a broad swath of sectors about the sources of attacks, the nature of attacks and the pattern of attacks, the more ultimate improvement will occur in the responsiveness and the defense of all sectors. Frankly, however, organizations are often hesitant to share this type of information. Some are concerned that information exchanged will not be protected and will subsequently be revealed. While true even with private-to-private sharing, this is especially true with private companies sharing information with public entities. Private organizations are concerned that revelation of the information will impact their reputation and the confidence of their customers – regardless of their industry. That is why the financial services industry along with other industries was supportive of the passage of HR 3523, the Cyber Intelligence Sharing and Protection Act, which, if enacted, offers additional protections and assurances to the confidentiality of shared information.

---

[2] The term *bot* is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a *botnet*. Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. (As defined by Microsoft ® Safety & Security Center at http://www.microsoft.com/security/resources/botnet-whatis.aspx)

It is important to recognize that the information sharing generally done with regard to cyber attacks seldom involves non-public, private information regarding individuals. We recognize that as HR 3523 was debated, the concern about protecting individuals' information and privacy was a legitimate concern raised by several Members of the House. As you consider future cybersecurity legislation, however, we do urge you to consider solutions to allow sharing of this type of information under certain circumstances in a manner that protects the rights of individuals, but facilitates their protection as well. There are legitimate reasons to share this information that benefits citizens. For example, a breach occurring at a payroll processor can result in cybercriminals obtaining the checking account information of individuals. Today, sharing that information with the financial institutions that hold those accounts is difficult at best. Sharing it, however, and sharing it quickly, would allow those institutions to take action to prevent fraud against their commercial and retail customers.

In closing, please accept my thanks for the opportunity to testify to the Committee. Cybersecurity is a vitally important issue for both the private and public sectors. Protecting companies, and more so, protecting their customers and our citizenry in general must remain key imperatives for us all. Further, protecting the infrastructures that support our economy is crucial to maintaining confidence and an operating global financial system. We commend the Committee for recognizing the importance of this subject and for your attention in supporting the strongest cyber defense for our nation.

###

Statement for the Record

by

Errol Weiss

Director of the Cyber Intelligence Center

Citi

Before the

House Financial Services Subcommittee on

Capital Markets and Government Sponsored Enterprises

Hearing on

"Cyber Security for the Capital Markets"

June 1, 2012

Good morning Chairman Garrett, Ranking Member Waters, and members of the Subcommittee:

My name is Errol Weiss; and I am the Director of Citi's Cyber Intelligence Center, which is responsible for collecting, analyzing, and exchanging threat intelligence in an effort to protect the Citi brand, global business operations, technology infrastructure and client trust against cyber threats world-wide. This morning I am testifying on behalf of the Securities Industry and Financial Markets Association (SIFMA) on how to best protect capital markets from emerging cyber threats.[1]

I. Introduction

SIFMA supports the goals of the Administration and Congress to limit cybersecurity threats to the American people, businesses, and government through a more integrated approach. The increase in cyber intrusions and cyber crimes in the past decade is cause for great concern, particularly to those in the financial services sector. SIFMA member firms are on the front lines defending against cyber threats to the financial markets and we take this role very seriously.

---

[1] The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

At the outset, we think it's important for Members of Congress and the Administration to understand the existing regulatory framework under which the financial services industry functions.

II. The Existing Cybersecurity Infrastructure of the Financial Services Sector

The United States has embraced a sector-specific approach to data security and privacy regulation for decades. SIFMA urges Congress to consider the unique position of the U.S. financial services sector in connection with the ongoing examination of the national cybersecurity framework. As part of the financial services industry, SIFMA members are currently subject to stringent laws and regulations on the protection of personal data, including the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA). These laws and regulations are reinforced by regular, pro-active review, and audited by highly specialized regulators that are supported by the Federal Financial Institutions Examination Council (FFIEC), an interagency entity that issues data privacy and cyber security guidance and monitoring procedures. As discussed below, financial services firms appreciate more than almost any other sector of the economy the importance of maintaining the confidentiality of customer information. The financial services industry is keenly aware of the consequences resulting from a privacy or security lapse, and has long played a leadership role in developing policies, procedures, and technology to protect customer data.

The financial services sector has had an effective and longstanding working relationship with the U.S. Treasury Department on cybersecurity since Presidential Decision Directive/NSC-63 was issued in May 1998. In response, the industry proactively formed the Financial Services Information Sharing and Analysis Center (FS-ISAC)[2] which began operations in October 1999. After September 11, 2001, and in response to Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector that could impact business continuity and resiliency. Citi was one of the founding members of the FS-ISAC and I am currently on the FS-ISAC Board of Directors. A key factor in the success of the FS-ISAC is trust. And trust takes years to develop. The FS-ISAC has worked hard to facilitate the development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations such as law enforcement, regulators, and intelligence agencies for over a decade. We cannot afford to weaken that trust.

In addition to the work and success of the FS-ISAC the financial services industry is already one of if not the most highly regulated industries from a cybersecurity standpoint. SIFMA members are currently subject to the FCRA, GLBA and the examination guidelines of the FFEIC. Since 1970, the FCRA has promoted the accuracy, fairness, and privacy of personal data assembled by "consumer reporting agencies" (CRAs), including data provided by a majority of SIFMA member firms. The FCRA establishes a framework of fair information practices that include rights of data quality, data security, identity theft prevention, and use limitations, requirements for data destruction, notice, user consent, and accountability.

---

[2] For an overview of the FS-ISAC's responsibilities and functions, please visit: http://www.fsisac.com/files/FS-ISAC_Overview_2011_05_09.pdf

The GLBA provides data privacy rules applicable to "financial institutions," a term defined broadly to cover entities significantly engaged in financial activities such as banking, insurance, securities activities, and investment activities. The GLBA imposes data privacy obligations such as the obligation to securely store personal financial information, and provide data subjects with notice of the institution's privacy practices and the right to opt-out of some sharing of personal financial information. The GLBA regulations also provide guidelines to financial institutions on appropriate actions in response to a breach of security of sensitive data, including on investigation, containment, and remediation of the incident and notification of consumers and/or law enforcement authorities when warranted.

Finally, many SIFMA member firms also follow FFIEC guidance and monitoring procedures. The FFIEC is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

The FFIEC also makes recommendations to promote uniformity in the supervision of financial institutions. In the area of cybersecurity and data breach protection, the FFIEC has published the following standards: FFIEC Interagency Guidelines Establishing Standards for Safeguarding Customer Information; FFIEC Interagency Guidelines Establishing Information Security Standards; FFIEC Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice; FFIEC Information Technology Examination Handbook (includes guidance and audit provisions of many of the requirements identified in the guidance documents referenced above).

III. Proactive Sector Initiatives

FS-ISAC Account Takeover Task Force

In 2010, the FS-ISAC formed the Account Takeover Task Force (ATOTF) as a result of continued concern and need for additional tools to help financial institutions and their customers combat online account takeover attacks. The ATOTF consists of over 120 individuals from thirty-five financial services firms of all sizes and types, ten industry associations and processors and representatives from seven government agencies. The ATOTF focuses on deliverables in three areas of effective cyber defense: Prevention, Detection and Response.

Some example deliverables and products produced by the ATOTF include:

Prevention

- Fraud Advisory for Businesses: Corporate Account Take Over, co-branded with US Secret Service, FBI and Internet Crime Complaint Center (IC3). The advisory is available here: http://www.fsisac.com/files/public/db/p265.pdf

- Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams, co-branded with FBI and IC3. The advisory is available here: http://www.fsisac.com/files/public/db/p264.pdf
- J1-Visa Money Mule Advisory
- Internet Auto Fraud

Detection

- Detection Whitepaper for financial institutions – Document focused on detection of account takeover victims.
- Techniques for recovering customers from ZeuS or other keystroke logging/man-in-the-middle Trojan infections and the exploration of third-party services with the goal of gathering elements of intelligence to enable better detection methods.
- Document Standard Set of Requirements and enhancements for alerting and security requirements for core ACH/wire transfer software providers.

Response

- Contact List, Procedures - This list provides financial institutions the information they need to report account takeover attacks via online banking to the Secret Service, FBI and other agencies, and a process for keeping the contact lists current.
- Form for Reporting account takeovers, including what should be submitted in the incident report and used for metrics to measure the success of the ATOTF.
- Actions financial institutions can take after an incident, communicated via FS-ISAC advisory notices.
- Internet Fraud Alert service from the National Cyber-Forensics & Training Alliance (NCFTA). This provides financial institutions with information for recovered credentials from the takedown of botnet command and control servers.
- List of Resources currently available for cyber crime and broad education so that financial institutions can leverage existing resources.
- Malware Submission method provides a process for sharing identified new malware with government/law enforcement agencies and anti-virus vendors.
- Redesign Suspicious Activity Report (SAR) Submission and Analysis Process by working with the Financial Crimes Enforcement Network (FinCEN) to give financial institutions and regulators more actionable information.
- Recommendations for reporting an account take over attack via SARs.

Finally, the ATOTF implemented a survey and polled member organizations regarding commercial account takeover to establish a baseline for Commercial Account Takeover attempts and losses. The surveys collected data in 2009, 2010 and the first half of 2011. The results indicate that financial institutions are doing a better job of stopping fraudulent transactions.

Botnet Takedown Partnership with Microsoft

FS-ISAC, in partnership with Microsoft and NACHA, announced on March 26, 2012, that they successfully executed a coordinated global takedown operation against some of the most notorious cybercrime operations responsible for online fraud and identity theft. The takedown was accomplished through coordinated legal and technical actions and disrupted massive botnets using the ZeuS and SpyEye malware families, striking a major blow against cybercriminal operators targeting the financial services sector's customers.

A video news release about the disruption, codenamed, "Operation B71", is located here at the Microsoft Digital Crimes Unit web page: http://www.microsoft.com/presspass/presskits/dcu/ . The takedown will help prevent online fraud and identity theft for consumers and businesses worldwide. Microsoft's investigation shows that approximately 3.6 million computers in the United States alone have been infected with the ZeuS malware.

This takedown was made possible through a successful pleading before the U.S. District Court for the Eastern District of New York on March 19, 2012, which allowed Microsoft, FS-ISAC and NACHA to sever the command and control structures of several of the most dangerous botnets running ZeuS, SpyEye and Ice IX malware. Because the botnet operators used ZeuS, SpyEye and Ice IX to steal victims' online banking credentials and transfer stolen funds, FS-ISAC and NACHA joined Microsoft as plaintiffs in the civil suit.

On March 23, 2012, Microsoft and co-plaintiffs FS-ISAC and NACHA, escorted by the U.S. Marshals Service, executed a coordinated physical seizure of servers in multiple hosting locations to preserve evidence for this case and seized hundreds of domain names used by the ZeuS, SpyEye and Ice IX malware to remotely command and control victim computers. Although it is not expected that this operation will completely destroy all botnets running ZeuS, SpyEye and Ice IX malware, or even that every botnet taken down in the operation will stay down permanently, this action is expected to significantly disrupt the cybercriminals' operations by increasing the risk and costs for its controllers to continue doing business.

Microsoft has stated that it will use the intelligence gained from this takedown to partner with Internet Service Providers and Computer Emergency Response Teams around the world to help remediate infected computers from the control of ZeuS, SpyEye and Ice IX, making the Internet safer for consumers and businesses worldwide.

Together, these aspects of the operation are expected to undermine the criminal infrastructure that relies on these botnets every day to make money and helps to provide new tools for the industry to work together to proactively fight cybercrime.

IV. The Threat - Hactivists, Organized Crime and Nation States.

Threats to the banking and finance sector come primarily from three groups – hacktivsts (on-line activists promoting a sociopolitical ideology), organized criminal gangs (committing cybercrime for financial gain), and foreign nation states / extremist groups (committing industrial espionage to gain competitive advantage or disrupt financial markets).

Hacktivism is a term used to describe motivated individuals and groups that use hacking techniques to promote a political ideology. While traditionally cyber based, in 2011, we witnessed hacktivist causes spill over into the physical world as well, causing disruptions and complicating business operations for many government and businesses, including SIFMA members. Starting as far back as 1994, hacktivists were using Distributed Denial of Service (DDoS) attacks to make internet sites and services unavailable to intended users. DDoS attacks have since become a staple hacktivist technique, resulting in lost revenue and reputational damage. In the past year, hacktivist activity has exploded, with malicious actors bent on retaliation against organizations that do not support their cause. Hacktivist tactics continue to include DDoS attacks and also include public exposure of sensitive internal information.

Sophisticated criminal organizations continue to target individuals and organizations with sensitive financial information. Once they are able to compromise a victim, criminals are quickly turning the stolen data into financial gain. The criminals operate a sophisticated and mature business, with a complete operating model that includes outsourcing of each discrete component of the underground ecosystem to specialists and experts around the globe. Criminals cooperate through the development of malware to evade anti-virus protections, the delivery of malware via targeting phishing emails and/or infected websites, stealing customer credentials and answers to challenge questions, takeover of on-line banking accounts, and movement of stolen money through a network of unwitting and/or complicit professional "money-mules" to the criminal syndicate often outside the U.S. in places like Eastern Europe.

Technically advanced and adversarial Nation States and extremist groups represent the third major threat to the banking and finance sector. Foreign economic collection and industrial espionage against the United States and other nations are conducted, to a large degree, in Cyberspace. Virtually every business activity and the creation of new ideas take place on the Internet. Malicious actors, whether they are corrupted insiders or foreign intelligence operatives, can easily steal and transfer massive quantities of data while remaining anonymous and nearly impossible to detect. Foreign operatives with motivation to steal sensitive economic information are able to operate in cyberspace with relatively little risk of getting caught.

The use of sophisticated malware, along with highly cooperative hackers for hire, makes it difficult to attribute responsibility for the entities behind corporate computer network intrusions. Foreign adversaries perform industrial espionage to target proprietary (and sometimes non-proprietary) company information they can use for their own gain. For a SIFMA member firm, foreign adversaries could be interested in information like client lists, merger and acquisition data, company information on pricing, and financial data. High technology firms may be targeted for new design information. Extremist groups use the same techniques to gain system access, but go a step further by using that access to cause disruption and/or destruction. As an example, recent DDoS activity against large U.S. member firms has been orchestrated by extremist and terrorist groups associated with foreign nation states.

V. Information Sharing

Despite the robust cybersecurity infrastructure that the financial services sector has established and the current ability to share information with our peers and others, SIFMA recognizes the need for expanded information sharing with government agencies, including greater private sector access to threat data from Federal intelligence and law enforcement agencies. Access to threat information must be administered in a manner that can provide broader cybersecurity protection without compromising ongoing investigations or the privacy of individual Americans. In addition, providing greater access to security clearances for private sector employees will increase the likelihood that cyber threat information will be distributed in a timely manner and handled properly.

While we support enhanced transparency and information sharing, we are concerned that if sensitive private sector information is shared with a government agency, it could be divulged to the public in response to a Freedom of Information Act (FOIA) request. Such disclosure could invite further attacks or create the perception that an institution is defending itself ineffectively. SIFMA believes that cybersecurity information shared with government agencies, including the identification of critical infrastructure, must be exempted from disclosure under FOIA.

Additionally, SIFMA believes government agencies should leverage ISACs and the United States Computer Emergency Readiness Team (US-CERT) to facilitate two-way and cross-sector public/private information sharing. We believe the ISACs should remain in place for mature sectors like financial services and we oppose any cybersecurity legislation that establishes a "National Information Sharing" clearinghouse, which will add layers of bureaucracy and delay information sharing with existing ISACs.

VI. Recent Cybersecurity Proposals

This past fall, the House Cybersecurity Task Force recognized that private-sector entities control the vast majority of U.S. information and communications technology and other critical infrastructure. These entities are in the best position to identify and defend against cyber-related threats. Owners and operators are, and should be, responsible for the protection, response, and recovery of private assets. Yet, there is widespread agreement that the public and private sectors need to work together, particularly when it comes to greater sharing of information in order to achieve enhanced situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats – while at the same time ensuring that personal information is adequately protected.

In the spirit of enhancing public-private coordination, several members of Congress drafted proposals to combat cyber threats to critical infrastructure; increase public/private information sharing regimes; increase cyber research, development and education; and update federal network security practices.

SIFMA is especially encouraged by the information sharing provisions contained within CISPA, introduced by Reps. Mike Rogers (R-MI) and Dutch Ruppersberger (D-MD)

SIFMA believes the sharing of information from government to industry has immense value but we are also supportive of the voluntary approach to information sharing from the private sector to the government. CISPA provides a solid framework and useful legal protections to encourage and permit the timely flow of actionable information. Creating an environment where cyber threat intelligence is readily available and shared is fundamental to any long-term endeavor to defend our country and make our markets more resilient.

As the debate continues in Congress, in addition to information sharing, SIFMA asks that Members keep the following principles in mind with respect to the following issues:

1. **Critical Infrastructure:** Several of the recent cybersecurity proposals include provisions that grant DHS the ability to designate an organization as a critical infrastructure operator and then regulate that system or organization. SIFMA believes that the financial services sector's current regulator is best-suited for the role of designating or regulating a critical infrastructure operator because they have a long history and are familiar with the complex operations of financial services organizations. The Treasury Department, as the Sector Specific Agency for the financial services sector, and the regulatory agencies through the Financial and Banking Information Infrastructure Committee (FBIIC), should determine if an institution in the sector is considered critical. The financial industry, like many other industries in the United States, is far too complex to be managed and regulated via a one-size fits all solution.

   Furthermore, when determining what constitutes critical infrastructure within a firm, the scope of critical infrastructure should apply to specific capabilities, processes, functions or business units and not to an entire firm or institution. It must be recognized that critical infrastructure is built within an ecosystem that includes commercial vendors and suppliers that contribute to the overall resiliency of the capability, process or function that should be protected. SIFMA supports enhanced supervision over service providers on which financial institutions depend (e.g., hardware and software providers, Internet service providers, etc.); however, such coordination may be better achieved by building on some of the existing mechanisms that seek to address these issues (e.g., Partnership for Critical Infrastructure Security).

   Building on existing mechanisms and organizations within the sector, we feel it is essential that the private sector have a prominent voice in the criteria that will be used to designate critical infrastructure. By leveraging the established partnership between the Financial Services Sector Coordinating Council (FSSCC) and the FBIIC, the experts can come together and determine what the criteria, metrics and thresholds should be to determine if a specific capability, process, function or business unit within the financial services industry is critical. Once those systems are denoted, leveraging and updating the existing rules in place that we as an industry already adhere to would make implementation and assessment as seamless as possible.

2. **Supply Chain:** SIFMA supports federal cybersecurity supply chain management and promotion of cybersecurity as a priority in Federal procurement. Other efforts to defend against cybersecurity threats will be lessened without financial support for the infrastructure necessary to implement a defense strategy.

3. **Law Enforcement:** SIFMA supports the strengthening and clarification of criminal penalties for cybercrimes. These improvements further bolstered by an increase in budgets and personnel for these purposes at law enforcement agencies will provide additional protection for consumers and financial institutions.

4. **Research & Development:** The development of essential technologies and improving federal systems are important efforts which should be supported. As DHS and the National Institute of Standards and Technology (NIST) pursue their research and development agendas, we hope to see substantial resource commitments and advances in these areas. We also support the improvement of the resilience and security of federal systems to further prevent cybercrime.

5. **International Cooperation:** Because cybersecurity is a global problem and cyber crimes frequently occur across borders, cooperation with international partners is critical to preventing, investigating, and prosecuting cyber crime. The U.S. should seek strong cooperation with foreign governments, international law enforcement agencies and policy making bodies, to improve cybersecurity. The U.S. should pressure foreign governments to enact effective cyber security legislation and demonstrate they enforce those laws by prosecuting and punishing individuals convicted of such crimes. If we do not work across borders on this issue our ability to prevent, defend and deter cyber crimes will be severely limited.

6. **Safe Harbor for Disclosure:** SIFMA members believe that the safe harbor provisions for cybersecurity reporting will be helpful for SIFMA members and provide much-needed extra protections for sharing information beyond what is currently available under Protected Critical Infrastructure Information (PCII) provisions. Financial institutions that cooperate with the government in cyber-threat sharing should receive liability and confidentiality protections. We are in support of both strong liability and confidentially protections with strong preemption.

7. **Education & Awareness:** Public education and awareness campaigns have been a critical method of limiting cyber crimes in the financial services industry. Both the Securities and Exchange Commission (SEC) and SIFMA members have promoted public awareness of the risk of disclosure of personal information for many years, and SIFMA supports the expansion of any such campaigns and promotions.

8. **Breach Notification:** SIFMA members believe that a single, uniform federal breach notification standard that preempts state law would help reduce administrative oversight, establish clear notification guidelines, and reduce consumer confusion. We support a notification standard that is based on risk-based assessments of actual or likelihood of harm, and allows for a reasonable investigation and mitigation period.

VII. Conclusion

SIFMA supports the efforts of the Administration and Congress to further protect the American people, businesses, and government from the increasing threat of cyber attacks and cyber crimes. As you can see, the financial services sector faces a number of significant threats and is currently tracking several of them, with a concern that they may materialize in the future. We have outlined a number of the actions that the FS-ISAC has taken on behalf of the sector to identify and mitigate threats that we are facing. In addition, the financial services sector already has a strong regulatory regime in place with its existing regulators. This oversight, as well as partnerships with industry bodies and software providers, allows us to proactively work to ensure that our systems are protected and that we maintain flexibility so that we can respond quickly when threats change.

Recent proposals are a good first step in addressing some of the issues and the four bills recently passed by the House address many of the principles we laid out earlier. The changes to the Federal Information Security Management Act (FISMA) that will drive improvements in federal systems, increase coordination between federal agencies around education, awareness, standards and talent development, and the reauthorization of the Networking and Information Technology Research and Development program (NITRD), will assist in helping America better protect its cyberspace. CISPA in particular will move us along the furthest by making the private sector aware of the threats that are out there and provide a framework within which we can confidently share information with the government.

The sharing of actionable and timely intelligence will allow the people with the greatest expertise in protecting their systems, many of them critical to properly functioning markets and the economy at large, the best chance of anticipating, protecting and defending their systems and networks from the individual criminals, criminal syndicates and nation states that seek to steal intellectual property, disrupt markets and do harm.

SIFMA members are accustomed to and fully supportive of protecting their customers' data, and, as partners and service providers, the data of customers of financial institutions worldwide. Encouraging effective data protection goes to the heart of SIFMA's mission of building trust and confidence in the financial services industry. Without effective protection of the personal data of our customers, financial institutions would lack the public trust that is so critical for their operation.

Testimony of James R. Woodhill
Advocate, Government and Public Relations
YourMoneyIsNotSafeInTheBank.org
Before the U.S. House of Representatives
Committee on Financial Services
Subcommittee on Capital Markets and Government Sponsored Enterprises

June 1, 2012

Chairman Garrett, Ranking Member Waters, and members of the Subcommittee, thank you for the opportunity to testify today on behalf of the current and future victims of commercial-account account takeover fraud.

My name is Jim Woodhill. In December of 2009, I was recruited by Avivah Litan of Gartner, Inc., the leading industry cybersecurity analyst, to bring this crime to the attention of the Congress. Ms. Litan knew me as the founder, a decade earlier, of Authentify, Inc., one of the now scores of security solution providers with offerings that address this specific crime. I am now the government and public relations advocate for YourMoneyIsNotSafeInTheBank.org.

I am appearing before you today because your money is not safe in the bank. At least it is not if you are an American church, school district, public library, or small business that banks online on a Microsoft Windows PC. Shockingly, as is an official banking industry policy the American Bankers Association (ABA) calls "shared responsibility"— should foreign cybercrooks' malware takes over your PC and then that PC tells your bank's Internet banking system to transfer all your organization's money to Romania, you are out the money stolen in that cyberattack.

This doctrine of "shared responsibility" is bankrupt as security policy and is politically illegitimate. It is also heroically bad public policy because the money being stolen is funding rapid advances in cyber-attack technology, and we are starting to see crossover between cybercrime and cyberattacks by nation state actors. What was a smallish crime of fraud two and a half years ago is now part of a full-blown national security crisis, which extends beyond financial services. For these reasons alone it is not enough to rely upon our country's diverse population of commercial online bank account holders to keep pace with this evolving threat. On October 7, 2009, even FBI Director Robert Mueller mentioned in a speech in San Francisco that he had stopped banking online because he did not believe *he* could do so securely. If we are to turn the corner, these crimes must be stopped by utilizing combinations of technologies that have existed for years.

The first known victim of this crime, a family printing-cartridge business in Miami, lost $90,000 in April of 2004. It was not the crime, but Bank of America's unwillingness to make good on the loss that ignited a media firestorm so intense, The New York Times was still running articles about the case eight months after the news broke.

The Lopez family filed suit against Bank of America in February of 2005. Thereafter, the bank finally compensated the Lopez family for their losses, nearly two years after the crime had occurred. By then, the regulators had already reacted to this crime. In October of 2005, the Federal Financial Institutions Examinations Council (FFIEC) issued guidance entitled "Authentication in an Internet Banking Environment", describing the crime of malware-based account takeover and instructing the F.I.s under its purview not just to adopt the fraud controls needed to prevent the crime, but to keep those controls updated as the cyber-threat landscape evolves. No more cases surfaced in the news in the next couple of years.

By late 2008, the criminals re-emerged with "ZeuS", a new generation of malware that was much more powerful, persistent, and could be wielded by a criminal with no technical background. Within a year Ms. Litan was so alarmed by the mounting losses and the banks' lack of response to them that she put me in touch with Brian Krebs of the Washington Post, who was, and still is, the lead reporter on the cybercrime beat. Mr. Krebs directed me to the Post's archive[1] of his stories about victims and put me in contact with a number of them. However, since our group launched http://www.yourmoneyisnotsafeinthebank.org[2], new victims have started approaching us directly.

One of the latest victims of this scheme to contact me is TRC Operating Company, Inc. of Taft, California, an independent domestic energy producer, which has since filed suit over its victimization by the ironically-named United Security Bank of Fresno just two weeks ago. Eastern European cyber-criminals attempted to siphon more than $2 million out of the company bank account.

The stories all sound the same. A small- and medium-sized enterprise that banks online at an American small- and medium-sized bank somehow ends up with malware on the Windows PC it uses for online banking. The typical transmission vector is a successful email "phishing" attack that gets an unwary user to open an infected attachment file or visit a compromised web site. However it gets on the user's PC, the "ZeuS Trojan" infiltrates the user's web browser and watches for online banking logons. If the bank's URL is one of those known to follow the "Krebs Rule", which employs fraud controls that are effective even if the user PC is totally under the control of the enemy, the malware gives up and its human master spends his time trying to infect other PCs. However, if the F.I. is one that does not follow this rule, the criminal uses his "Man-In-The-Browser" attack kit to either capture the customer's logon credentials for separate use, or to actually hijack the customer's validly authenticated online session and use it to transfer money to accounts controlled by the criminal. While all of this is happening, what the user sees on his screen gives no hint that such is going on behind the scenes.

Even today, 70% of the time such an attack is conducted, the F.I. learns of it from its customer, rather than detecting it itself. Thousands of American organizations have been the victims of online bank robbery, and over 500 have lost money that was not reimbursed by their bank. Online bank robbery became a much more lucrative crime than physical bank robbery years ago.

---

[1] Washington Post Security Fix
http://blog.washingtonpost.com/securityfix/archives.htm

[2] http://www.yourmoneyisnotsafeinthebank.org

Dismayingly, neither the FDIC nor law enforcement knows for sure how many attacks there are and how much money in total has been lost, much less the split between the victim and the bank. Many banks do the right thing and cover such losses completely, though others do only partially—just enough to keep the victim from suing. Brian Krebs believes that only a fraction of account takeover incidents are reported to law enforcement.

At its Symposium on Combating Commercial Payments Fraud[3] held by the FDIC on May 11, 2010, the word "crisis" was used by both FDIC and law-enforcement officials. Those FBI agents stated that they were investigating 250 cases at that time, and the rate of growth they were seeing in victimization was 5X every twelve months. The estimate they offered was $70 million lost by commercial victims as of that date. In Assistant Director Snow's testimony, he stated that the FBI was investigating over 400 cases of account takeover fraud involving the attempted theft of over $255 million, resulting in the actual loss of approximately $85 million.

All of the victims of this crime, which is also referred to as "account-takeover fraud" or "ACH fraud", have gone through the same stages of a special grief process:

SHOCK--that their money could be stolen electronically

DENIAL--they just can't believe the official policy of America's banking industry is "shared responsibility", which in practice means "no responsibility" for keeping their organization's deposits safe, even though federal law forces them to take full responsibility for personal accounts.

ANGER--Why didn't my bank call me? I get calls all the time about charges on my credit card! Why won't they take responsibility? They urged me to sign up for online banking, and claimed it was safe! You mean "FDIC Insured" does not mean I will get my money back either? How could my PC have gotten infected? I run Norton anti-virus and update the product four times a day!

BARGAINING--trying to cut a deal with their bank to get an acceptable percentage of money back.

The last stage of the normal human grief process is commonly termed "ACCEPTANCE". Well, there is never any "acceptance" by the victims in these cases. Instead, there have been about a dozen lawsuits by victims who still had the means even after they were robbed. However, other victims simply went bankrupt. That would have been the fate of Karen McCarthy's Little & King, had I not extended a $100,000 loan to it. It was and is a great little business. It has made every payment on time, with interest. But without my help, it would have died, forcing the family it was supporting to pull its two kids out of college and lose their house. Mrs. McCarthy's husband was one of those brave New York firemen badly disabled responding to 9-11.

---

[3] Symposium on Combating Commercial Payments Fraud. FDIC. May 11, 2010. http://www.fdic.gov/news/conferences/2010_fraud/agenda.html

Since the original "Lopez" case, a number of these crimes have ignited additional media firestorms. One such case is PlainsCapital Bank vs. Hillary Machinery, Inc.[4] in early 2010, the bank filed suit against the victim of an account takeover. I have accumulated almost 5,000 news stories and technical articles on this crime, comprising almost 2 gigabytes of data. Never have I seen anyone outside of the financial services industry publicly defend the notion that banks are not responsible for keeping their depositors' money from being stolen. How can security measures and policies be "commercially reasonable", when, if the customers only knew what these policies were, the organization would have no customers? The ABA's arguments defy the common sense of average citizens, not to mention their sense of right and wrong.

It also defied the common sense of Senator Chuck Schumer, who, on September 29, 2010 introduced S. 3898[5], a partial extension of Federal Reserve Regulation E to cover state and municipal accounts.

That banks are not responsible for safeguarding their depositors' money from risks that have not even been disclosed to those depositors is a position unlikely to be sustained in the courts. Responsibility for the safety of bank deposits and the terms of the account agreement between bank and customer are governed by federal legislation and regulation, state contract law (specifically Section 4(a) of the Uniform Commercial Code (UCC)[6]).

For individual accounts, which are tied to a Social Security Number, there is no ambiguity. The Electronic Funds Transfer Act of 1978 (EFTA)[7], whose regulatory perfection is Federal Reserve Regulation E, commonly known as "Reg E", requires financial services institutions to make good on any losses, even if the user posts his online banking userid+password on Facebook. However, EFTA was explicitly a *consumer* protection act. EFTA did not say banks are *not* liable for safeguarding commercial accounts, those under a Federal Employer Identification Number. It was simply silent on the matter.

---

[4] PlainsCapital Bank vs. Hillary Machinery, Inc.
http://dockets.justia.com/docket/texas/txedce/4:2009cv00653/120329/

[5] S. 3898
http://www.govtrack.us/congress/bills/111/s3898

[6] Uniform Commercial Code Section 4(a)
http://www.uniformlaws.org/ActSummary.aspx?title=UCC%20Article%204A,%20Funds%20Transfers%20(1989)

[7] Electronic Funds Transfer Act of 1978
http://www.fdic.gov/regulations/laws/rules/6500-1350.html

Account takeover fraud loss liability is therefore governed by the contracts between the parties. However, these contracts must conform to the Section 4A of the Uniform Commercial Code (UCC) of whatever state the contract says its law will apply. Section 4A mandates that access to funds must be safeguarded by a "security procedure", and said procedure must be "commercially reasonable".

What is and is not a "commercially reasonable security procedure" is, therefore, the central subject of all the lawsuits. However, other causes of action can, and have been brought, including the argument that under the common law, banks are responsible for keeping their depositors' money from being stolen. "Commercially reasonable" is a legal term of art whose meaning is analyzed in depth in "The Commercial Reasonableness of Bank ACH Security Procedures"[8] by Brad Maryman and Dr. Stan Stahl. It was also the subject of a mock trial at the 2011 RSA Conference entitled, "Whose Fault Was It That I Did Not Know You Were You?"[9], which was presided over by federal magistrate John M. Facciola. In that session, as in the real case of PlainsCapital Bank vs. Hillary Machinery, Inc., I was expert witness for the victim *pro bono*. Of course, I could not speak to the meaning of the legal term "commercially reasonable" in UCC-4A, as we had two top lawyers argue that. My role as a security expert was to testify that the online banking fraud controls of the bank in this hypothetical case, even if they met the test of "commercially reasonable" in some abstract legal way, had not provided what a "reasonable man" would consider "security" in the technical sense, nor did they comply with the 2005 FFIEC Guidance. Given that this was a jury trial, and the jury was the audience, the victim won easily.

In any such real lawsuit, the F.I. would be well advised to avoid a jury trial. Were I a lawyer, I would not take the case of the bank. But if I had to, I would have to challenge the seating of any juror who had any interest in a commercial bank account, or attended a church, had kids in a school, or lived in any local political entity, because organizations of all these types and more have been victimized. I would demand that any judge with such conflicts recuse themself. It is likely that there is no judge in America that would pass such a conflict-of-interest test, and perhaps no potential juror.

---

[8] "The Commercial Reasonableness of Bank ACH Security Procedures" http://www.citadel-information.com/wp-content/uploads/2011/04/commercial-reasonableness-of-bank-security-procedures-101207.pdf

[9] "Whose Fault Was It That I Did Not Know You Were You?" http://cornerstonesoftrust.com/presentation/whose-fault-it-i-didnt-know-it-wasnt-you-panel-discussion

Right now, the official lawsuit tally is one finding for the victim and one for the bank, with three settled on terms favorable to the victims and at least seven ongoing. Besides the case brought by the Lopez family, there have been at least two other lawsuits where the bank settled immediately after hearing what the judge in its case had to say, in addition to his or her denial of the bank's motion for summary judgment. At the 2012 RSA Security conference in March, which was attended by 22,000 security professionals, there was a follow-on session to our mock trial back in 2011. At this new session, a panel of top cyberlaw experts, led by U.S. federal magistrate John Facciola, predicted that, considering that the 2011 FFIEC Guidance was now in effect, going forward, such cases would increasingly end with summary judgment for the plaintiff.

The one case that was "won" by the bank, PATCO Construction vs. People's United Bank[10], the judge had to overlook the fact that Oceans Bank, which was acquired by People's United Bank after the crime but before the lawsuit, had ignored the fraud alerts sent to the bank by its outsourcer. The outsourcer had scored the bogus transactions' risk at "800" versus at most "8" for previous transactions. You are hearing me correctly. In the PATCO case, all the technical fraud controls necessary to have saved PATCO's money were already in place and operating. Nothing new needed to be implemented or even understood. All the costs were already being billed by the processor to the bank. As I have said previously, technically, this is a long-beaten problem. I put the word "won" in quotes, because PATCO Construction's attorneys estimate that Peoples United has to date spent over $1 million in legal fees to avoid reimbursing a $360,000 loss, defending its policy of "shared responsibility".

It is precisely this type of event, yet higher profile, which could spark a mini "run on the banks". Depositors would flee from any bank without proper security measures to those banks that provide adequate protection and/or absorb any losses. As soon as anyone with an interest in a small- and medium-sized enterprise learns of the threat from malware-based account takeover and visits YourMoneyIsNotSafeInTheBank.org, they are urged to take a letter demanding liability disclosure to their bank. If the customer is not satisfied with their bank's protection, they are advised to move their accounts to a bank where they are protected. To know about this attack is to be very quickly safe from it.

To bring this point home, any member of this Subcommittee whose campaign fund banks online could see its funds vanish into eastern European bank accounts overnight. Rest assured, Mr. Chairman and Ms. Ranking Member that at the Symposium on Combating Commercial Payments Fraud conducted by the FDIC on May 11, 2010, Bryan Nash of Illinois-based McHenry Savings Bank, who led the panel of bankers who vigorously defended the ABA's doctrine of "shared responsibility", replied to my specific question that if the campaign funds of a member of the House Committee on Financial Services were ever stolen, your campaign would be fully reimbursed without the Member even having to ask. The campaign treasurer involved would have some shocking and scary moments, and it might take a few days for your campaign's money to be "restored" but quite soon you would be made whole. Yet again, who's to say what the criminals are doing with their loot.

---

[10] PATCO Construction vs. People's United Bank
http://voices.washingtonpost.com/securityfix/Complaint%20091809.pdf

It is only the Hillary Machinerys, PATCOs, and Duanesburg School Districts that are at risk of total, or at least partial loss. Indeed, at Cherry Hills, NJ-based TD Bank, if you are the Town of Poughkeepsie, NY and you have $378,000 stolen by cyber-thieves, you will be fully reimbursed, at least after your state's senior senator introduces legislation to extend Federal Reserve Regulation E to cover municipal accounts. But if you are tiny Little & King on Long Island, banking at that very same F.I., your $120,000 loss will be allowed to bankrupt you.

I am here to argue against either the victims or small- and medium-sized banks having to bear the losses or the risk of losses itself. Note that it does not matter whose pocket the tens of millions currently flowing overseas from U.S. bank accounts comes. It's helping to fund the R&D efforts of criminal masterminds with whom a little money buys a lot of software development. That money is also funding the building out of an entire criminal economy, on which today one can buy, for example, the full identities, including Social Security Numbers of thousands of Americans over the age of 65 and then commit Medicare billing fraud, or any other species of identity theft.

Who in the world could defend the position of the ABA on account takeover, especially when the continued flow of victims' money overseas is funding the advancement of such destructive software? The lack of support among the public for the ABA's position makes it particularly ironic that I, the advocate for the victims, must speak in support of it.

On April 19, 2010, I met with Ms. Feddis and her partner Doug Johnson at ABA headquarters. They had told members of this Subcommittee, who had inquired after I met with them, that extending Regulation E to cover commercial accounts would "drive community banks out of online banking." At the end of a 2-hour meeting, I came away with the realization that they were correct. America's small- and medium-sized banks cannot take on liabilities that they lack the skill and, just as importantly, the scale to manage.

I also realized at that meeting that government affairs people, even those working for the ABA, are not necessarily well informed on the technical capabilities of the latest-generation fraud controls. They claimed that there were no purely technical solutions to this crime. That was only true if one would argue that Oceans Bank had no technical solution in place because it had not staffed the business process (examining the fraud alerts sent to them by their processor) that supports that technical solution. That's a stretch. In any case, Mr. Johnson was working his heart out to educate his membership about ZeuS and its cousins so they could stop these attacks he simultaneously stated they were not responsible for.

My conceding the correctness of the ABA's position that America's small- and medium-sized banks cannot bear the risk of this crime does not mean I can support their doctrine of "shared responsibility". That America's small- and medium-sized banks do not have the cybersecurity solutions and skills, nor the financial scale to bear the risks and responsibilities associated with online banking (which, of course, they probably *do* have under existing law), does not mean that their small- and medium-sized enterprise customers can either. By 2008, the firewall and anti-malware products that had protected them in 2005 had been beaten by the fraudsters and remain impotent. In any case, given that hospitals cannot move the needle on getting doctors to follow hand-washing guidelines, the notion that 20+ million small organizations are going to execute cybersecurity measures flawlessly day in and day out is preposterous. There are offices within the Congress that have had to have every single Windows PC replaced twice now because they had become so deeply infected by malware that no remediation was possible.

Let me emphasize that this is not a criticism of the management teams of America's small- and medium-sized banks. It was patently obvious when I met with the ABA that in spite of the FFIEC's Guidance and even the FDIC's August, 2009 Special Alert[11], they had not heard of this crime. As I will show below with an example from gastroenterology, information moves through a profession at a pace that can only be characterized as glacial, outside of situations that no one could wish to happen.

PlainsCapital Bank vs. Hillary Machinery, Inc. was a case in point why the FFIEC had to issue its supplemental Guidance in June of last year. PlainsCapital employed "two factor" authentication, but it was a fake version that amounted just to a few additional passwords, called "challenge questions". No security expert would have mistaken challenge questions for the "second factor of authentication" called for in the 2005 Guidance. However, back then the regulators had bent over backwards to be "technology neutral" in their recommendations and some security startups took advantage of that and the banks' lack of expertise to sell them "two-factor" authentication that was really a single factor twice.

Let me also explain that those banks that were aware of this crime but did not have deep in-house cybersecurity expertise were hampered in responding by a subtle intellectual confusion that the regulators inherited from my own information security industry. The problem can be seen in the title of the October 2005 FFIEC Guidance, "Authentication in an Internet Banking Environment". Back then, session-hijacking attacks were unknown, so the focus was on preventing attackers from using malware to steal logon credentials and then use them to impersonate the victim from their own PCs. This kind of attack was what was used to steal, in early November of 2009, over $800,000 from the accounts of Plano-based Hillary Machinery, Inc. at Dallas-based PlainsCapital Bank (PlainsCapital managed to claw back $600,000 of that sum). Note that this is the infamous case where the bank sued the victim, in spite of PlainsCapital's CEO having received the FDIC's Special Alert on August 26 of that year and also, in spite of being out of compliance with at least the spirit of the 2005 Guidance, because PlainsCapital's "two-factor" authentication technique was based solely on "Things You Know" that could be stolen in a single malware-based attack and used elsewhere.

---

[11] FDIC Special Alert. August 2009. http://www.fdic.gov/news/news/specialalert/2009/sa09147.html

At the 2010 FDIC Symposium, I spoke with a number of community bankers, including Bryan Nash of McHenry Savings Bank. They were all earnest, salt-of-the-earth people who would not buy into a doctrine as commercially and politically toxic as the ABA's "shared responsibility" (for account takeover fraud) if they weren't being squeezed by forces they could not manage. I think it is very important to note that ZeuS emerged at about the time Lehman Brothers' collapse plunged the entire world economy--via its banking system--into a crisis that lingers to this day. Community Bankers were hit with huge new FDIC assessments to bail out a small number of their foolish (or worse) lenders to the residential real estate market, not to mention having the mountain of financial industry regulations they have to comply with greatly grow in height. They had a lot more on their plate than remote-sounding cybersecurity threats.

The specific fear bankers articulated privately is that if they signed up for their processors' advanced fraud controls, the small- and medium-sized enterprises that bank with them would just "take their business down the road to a competitor that does not impose such hassles on them." As a security guy, I was baffled by this statement, and had to struggle to understand the world from the point of view of the CIO of a community bank. However, at the FDIC Symposium, Murray Walton, Chief Information Security Officer (CISO) of Fiserv, one of the largest processors told the audience that he must have pitched "two dozen" bankers on his company's advanced fraud controls, and made no sales because the bankers had never heard of the problem and/or did not believe it could happen to them. All of them subsequently had victims. His processor had the needed solutions, but it could not force customers to adopt them.

The deep intellectual problem that community bankers had inherited from the security community via the FFIEC Guidance was that the answer to account takeover / ACH Fraud was better online banking user authentication at logon. The very name of the FFIEC Guidance embodies that subtle flaw in thinking. And yes, it's a tremendous hassle for people to have to have an RSA SecurID on their keychain and to use it every time they log on even just to see if a check cleared. Mr. Nash and his fellows assumed that I was now also asking them to demand that their SME customers go through an extended "transaction confirmation" process for every online payment they do.

I realized that "transaction confirmation" was the term of art that had to replace "user authentication" in the conversation about account takeover. But the only transactions that had to be confirmed were "ADD PAYEE" and change-of-account-control information (e.g., the contact phone number on an account). These are very, very rare transactions for the typical online banking customer, yet criminals cannot make off with a customer's money by paying its phone bill excessively. All the crimes involve adding new payees overseas, or at least adding domestic U.S. "money mules" to the organization's payroll and then giving them incredibly large hiring bonuses. None of the crimes have been at all subtle. At Choice Escrow of Springfield, Missouri, BankCorp South allowed the entire contents one of its title accounts to be transferred to a new payee on the island of Cyprus on March 17, 2010, it helpfully loaned the victim $90,000 so the overdraft the cyber-bank-robbers had created would not prevent the transfer from happening. Choice has sued. BankCorp South, another F.I. that used one-factor security twice and calls it two-factor, has replied to the suit that their online banking security measures were completely adequate, and, anyway, they have abruptly and massively upgraded them! Again, I cannot speak to "commercially reasonable". I have come to talk to you about "security" and how the victims our little organization represents did not have the benefit of it at their banks.

Ironically, the regulators know that the key transaction that requires many-layered defense is "ADD PAYEE", they were just not clear about that in their 2011 Guidance[12]. Studies by Javelin Research of customer acceptance of having to take the occasional call to verify, for example, that Duanesburg School District really did intend to add twelve new payees in Russia and the Ukraine over a long holiday weekend, increase customer satisfaction, not decrease it. These findings were presented at the FDIC Symposium, but the speaker and the regulators were thinking of single-digit numbers of ADD PAYEEs a year, while the bankers were thinking in terms of the hundreds or perhaps even thousands of logons and payments they did. The latter is literally three orders of magnitude greater than the former, and would indeed represent imposing an unbearable amount of security hassle upon online banking customers.

If the FFIEC had issued Guidance on how to stop account takeover five years earlier and the technical solutions were easy and cheap, then how can I say that the banks can't be held responsible? Here, I am making a "public policy" argument not a legal one. At a conference at Brown University that I attended just last month, one of the most cybersecurity-savvy members of the House, Congressman Jim Langevin, went out of his way to observe that America needs 20 to 30 thousand fully-technically-qualified "cyberwarriors". He then stated that we have perhaps 1,000 today. When the FFIEC Guidance was issued, we had a small fraction of that and quite a few more F.I.s than we have today. America's community bankers are not cyberwarriors, nor can they hire cyberwarriors. It's one field in which the unemployment rate is zero.

Security experts could cite your (or the ABA's) chapter and verse about how account takeover was a beaten problem, technically, back in October of 2005 when the regulators first issued Guidance warning of this problem and advising America's F.I.s on how to keep it from happening. Faithful adherence to that original Guidance by one as skilled in the art of cybersecurity as one of Rep. Langevin's 1,000 cyberwarriors, using the security solutions available back then, would have thwarted 100% of the attacks whose details have been made public to date. Today's security solutions are inexpensive, quickly implemented, cheap to run, and enjoy high customer acceptance. If the "layered security" called for in the 2005 FFIEC's Guidance is implemented using information security best practices, the current solutions are more than sufficient. The root cause of crime is "criminals", and criminals are not like nation states. They are profit-motivated. While they will never go straight, they will switch to some other crime once stealing $1 starts costing $10.

---

[12] FFIEC 2011 Guidance.
http://www.ffiec.gov/press/pr062811.htm

The next attack is always right around the corner. Organizations big enough and smart enough can always withstand the attacks and protect their customers. But such organizations will always be few in number compared to the total size of the membership of the ABA. Over time, small organizations could gain in cybersecurity expertise, but over that same period of time the attack landscape will grow as much or even more complex.

Should that little northeastern bank have already been moving? On August 26, of 2009, the CEO of every FDIC-insured institution received a one page Special Alert from the FDIC specifically warning about the epidemic of account takeovers and warning them to take appropriate measures to safeguard their customers' funds. Yet, the following April, I spoke with the CIO of a tiny (just 200 commercial accounts) community bank on whose board he then sat. The CIO had never heard of the attacks mentioned in the 2005 Guidance or the 2009 Special Alert either. Despite the efforts to educate him by the FDIC and also his current outsourcer, who had the necessary security measures in his current online banking platform, my description of the attacks and recommendations on how to stop them were completely new news.

Was this CIO incompetent? Not a bit. I know talent when I talk to it, and also commitment. Cybersecurity is just too big and complex for small organizations to deal with.

That we have no hope at all of meeting the threat of account takeover by educating community bankers to be cybersecurity experts is nowhere more easily visible than in medicine.

On September 28, of 2006, the Centers for Disease Control published a bulletin on its web site that said, "Good News - A Cure For Ulcers!!"[13] This news item breathlessly announced that:

---

[13] "Good News – A Cure For Ulcers!!" Centers for Disease Control. September 28, 2006 http://www.cdc.gov/ulcer/consumer.htm

> Recently, scientists have found that most ulcers are caused by an infection. With appropriate antibiotic treatment, your ulcer - and the pain it causes - can be gone forever!

A little digging finds that "recently" meant that two Australians had won the Nobel Prize in Medicine a year earlier for this discovery that they made in 1981 and about which the paper that won them the Nobel was published in 1985. Note that the number of gastroenterologists in America is about the size of the membership of the Independent Community Bankers of America (ICBA). Unlike the bankers, however, treating peptic ulcers is a gastroenterologist's core business. They are under a continuing medical education mandate to keep their licenses. Still, 20 years is the typical amount of time it takes to ripple a change in the standard of care through a medical specialty, even when the stakes are life or death. I will circle back to medicine because it offers the one acceptable model I have been able to find for how the learning curve of a professional specialty can be accelerated.

Again, I was founder and chairman of a company that had one of the solutions, yet a paper had been published by the University of Mannheim (Germany) a year before I was contacted about the crime wave, which analyzed the emerging ZeuS malware-based attack kits. While I was just on the board of a solution provider, information security was my field. I had a 40-year career in enterprise software with the last 15 focused on information security. Can we ask a Duanesburg School District or a Hillary Machinery, Inc. to do better than I did? We cannot even ask this of a McHenry Savings Bank. Members of the subcommittee: a number of you heard about this crime for the first time from me in early- to mid-2010, yet two of you had victims in your district after this time.

I see public health's experience with using education and awareness for infection control repeating in our experience with the Conficker worm, which was first identified in November of 2008. The count of infected PCs is once again on the rise after being beaten back for a time by the Conficker Working Group and updated antimalware solutions. Conficker propagates by exploiting weak passwords on administrator accounts. Efforts to educate users to employ strong passwords predate the widespread commercial use of the Internet itself. If "education" and "awareness" efforts could accomplish anything at all with end users, there would be no weak passwords out there to be exploited. Alas, there are millions and millions of them on devices as varied as PCs, servers, and routers.

The 112th Congress' work on cybersecurity is encouraging. In the House's First Session, the cybersecurity task force, led by Congressman Mac Thornberry, led the way by synthesizing the best thought and opinion from the public and private sectors to lay out a roadmap for thoughtful legislative action. But in 35 hearings in the House alone, experts from both the public and private sector, while specific about the threats and the magnitude of the dangers, have been vague about solutions. I will be specific about the solutions I recommend to beat account takeover, but they will not work well in isolation.

I believe that they will be most effective if implemented as part of a comprehensive national cybersecurity strategy.

On November 22 of 2011, the Administration released its Comprehensive National Cybersecurity Initiative[14] (CNCI) which laid out three goals--establish a front line of defense against today's immediate threats, defend against the full spectrum of threats, and strengthen the future cybersecurity environment--and 12 separate initiatives to further these three goals. I tried to fit my proposal into this strategic framework.

In my view, to make cyberspace a "safe neighborhood", a comprehensive cybersecurity strategy for the U.S. would have four elements:

1) Harden American IT assets against cyberattack. The single most important thing we need to do is find a way of getting Norton (Symantec) and McAfee anti-virus products actually protecting again, along with the products of their 29 competitors. I have a specific proposal to accomplish this that I have been trying to interest the incumbent vendors in.

2) Make the work of cyberdefenders and fraud-fighters easier. Chairman Mike Rogers' Cyber Intelligence Sharing and Protection Act (CISPA) is an important step in this direction, but there are many more I could propose.

3) Determine the best use of government resources, especially those of law enforcement, in accomplishing the above two goals. The way many victims of account takeover have learned that they were being robbed is that they got a call from Washington Post reporter Brian Krebs, warning them that at that very moment, the cyber-crime was in progress. Brian somehow learns of these crimes in real time by monitoring ICQ (an Internet protocol used for chatting) traffic, yet this is much more useful and leveraged work than spending years trying to slap handcuffs on some kingpin in Ukraine.

4) Implement a decisive solution to the problem of "identity". The intersection of "identity" and "public policy" is the most intractable part of cybersecurity because we have not solved it in physical space, so there is nothing in place to be extended into cyberspace. I sketched out a solution, in response to the Financial Services Committee's hearings on FACTA and identity theft, which I came to call the Personal Identity Control System (PICS). Unfortunately, even though the PICS is simple at its core, defining its edges is much more difficult. However, we won't be secure in physical space, much less cyberspace, until we have something like the PICS.

---

[14] "Comprehensive National Cybersecurity Initiative" http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

It may sound strange that America needs to articulate "we must stop our churches, school districts, and small businesses from being robbed" as part of a new cybersecurity strategy, but I am offering this testimony because this has not yet been accomplished. Achieving this will, as I expand upon below, require moving the risks and responsibilities associated with operating in cyberspace to the entities most able to bear and mitigate those risks. It will also require, however, making the jobs of American cyberdefenders much easier and the jobs of foreign cyberattackers much harder, hence my brief mention of needing an overall strategy for security in cyberspace.

Let me now speak specifically to stopping malware-based account takeover attacks by a date, if not by the end of this year, certainly by the end of next.

While there are a lot of people involved with cybercrime, at the core there are a small number of hacker geniuses in Eastern Europe, China, and elsewhere, on whose innovations the entire criminal and nation-state cyberattack ecosystems depend. Any effective strategy for making cyberspace a safe neighborhood will require a larger, but still relatively small, number of cyber-geniuses on our side to defend all our IT assets. In the words of Rep. Thornberry and also Senator McCain, we need "active defenses" in cyberspace.

Community banks are not just an important part of the American economy; they are an important part of American society. They are small enough to actually know their customers, and make a living out of making loans to productive enterprises, rather than having to rely on a few large banks. Their management must spend all of its time thinking about expanding its financial assets (loans), not defending its cyber-assets.

Let me specifically speak to extending Regulation E to commercial accounts. My meeting with the ABA convinced me to oppose that solution. This does not mean I am not appalled by the doctrine of "shared responsibility" they attempt to defend. It does not make even commercial sense. In a free-enterprise system, companies like the ones I started got paid for taking on customers' responsibilities and discharging them better/faster/cheaper than our customers could do themselves.

Fortunately, the typical F.I. that is too small to do cybersecurity is also too small to actually run its own online banking information technology. At least 5,000 American small- and medium-sized banks outsource online banking to one of only 13 online banking platform vendors, or "processors". All of these organizations have the characteristics of an organization to which the risk of account takeover and the responsibility to stop it can be transferred:

- They run the IT on which online banking is actually conducted, so they are positioned to install and use the security solutions that have already been proven in the field as able to stop this crime. Indeed, some of them, at least on some of their online banking platforms (many processors have more than one), have already implemented the necessary layers of security solutions that have been proven in the field to defeat commercial-account online banking funds transfer fraud, and they have been trying to get their customers to adopt those solutions for years now.

- They are small enough in number that they can acquire the necessary expertise to understand the cyber-threat landscape they face and track its evolution.

- They have sufficient capital to take a few losses, and they host enough large accounts to attract the attention of giant insurers who are already in the cyber-loss business, should they feel they need to lay off some of the risk, rather than being self-insuring.

- They are large enough to hire staffs to do forensics on novel attacks.

- They can establish and maintain working relationships with national law enforcement agencies such as the U.S. Secret Service and the FBI, who have the jurisdiction and resources to pursue the criminals behind attacks.

- They stand to profit from protecting their banking customers and their account holders. Commercial-account online banking funds transfer fraud losses are much greater than the cost of the security solutions, so it offers the processors the opportunity to profit at the cyber-criminal's expense. Indeed, many of the processors are already trying to get their customer banks to buy advanced security solutions from them, but the customers just don't understand the threat. Right now, the fraud losses are higher than the fraud control costs needed to stop them, so this is an opportunity for money currently ending up in the pockets of the criminals to find its way to the bottom lines of the processors.

- They stand to lose from *not* protecting their small- and medium-sized bank customers' online banking customers, because if commercial-account online banking funds transfer fraud is not stopped, the word would eventually get around that small- and medium-sized enterprises' money is not safe in the banks who are the processors' customer base, and those SMEs would move their accounts to large banks who run their own online-banking IT and who put their money where their fraud controls are.

- They all compete for customers across our entire nation. This reform will enable them to start competing on the basis of cybersecurity effectiveness, fraud control cost, and minimum end-customer security hassle along with today's competitive factors.

The processors own the server side of online banking, where the overall business processes by which funds are transferred can be protected against attack. As Congress has heard from witness after witness in hearing after hearing in the last two years, there are no reliable user-client-side solutions. While "good cyber-hygiene" might stop 85% of individual attacks, as documented in Rep. Thornberry's task force report, the bad guys have unlimited "at-bats" with no "called-strikes". The way they work is to try the oldest and simplest attacks first, while resorting to valuable "zero-day" (previously unknown) Windows exploits only when easier/cheaper attacks fail and the target is valuable enough. A relatively small number of them can force us to try to defend tens of millions of attack points. Stopping 85% of the attacks will not protect 85% of the targets. The bad guys keep escalating.

All the client-side anti-virus solutions were beaten years ago. All the victims I spoke with had firewalls in place and they were running anti-malware solutions with up-to-date signature. It did not save them from ZeuS. All such products are now part of the test suites for the malware makers, and they keep working until their new version defeats them all. The individual small- and medium-sized enterprises are helpless before attacks by which even the laboratories that design America's nuclear weapons have been penetrated.

On April 21 of 2011, Gartner release a research report entitled "The Five Layers of Fraud Prevention and Using Them to Beat Malware"[15]. Those in charge of running online banking IT need only get a copy and line up its recommendations with the enhanced Guidance the FFIEC released on June 28, 2011 plus its original 2005 Guidance.

A useful goal of this effort is to bring the losses to account takeover down to zero without future Little & Kings or McHenry Savings Banks having to even know that there is (or rather "was") such a crime.

I have nothing against user awareness. I like the idea of an informed citizenry. I just insist, as the designated advocate for the victims and de facto advocate for our small banks, that they all get to live in a safe cyber-neighborhood. I lent Karen McCarthy's company $100,000 to keep it from going bankrupt when TD Bank let cybercriminals make off with that much of Little & King's money. But before I transferred the funds, I made sure that she switched to banking in the same place I have always had my own commercial accounts, an institution that requests to remain nameless. I have made the same demand of any other entity to whom I have extended loans.

Why would a bank that has invested in industry-leading technical controls and fraud control expertise not want its name mentioned? It's the reason that no U.S. bank competes on keeping SMEs' money safe in the bank. They don't refer to the eastern European criminals as being "the Russian mafia" for nothing. The web sites of more than one U.S. money-center bank have been knocked offline by DDoS (distributed denial-of-service) attacks already. None of the banks with mature fraud controls is willing to wave that particular red cape in front of the foreign criminals.

How can we affect this transfer of risk and responsibility from potential victims to the actual IT operators? In my opinion, regulation should be a last resort. When I studied this crime for the first time, my first thought was to require disclosure--just require that the risk of online banking be disclosed to the small- and medium-sized enterprise customer, and have them agree in writing to take the losses if their PC is hacked. However, it is hard for me to see this requirement doing anything but generating a flight to safety by the depositors and/or a flight from offering online banking by small- and medium-sized banks. I would greatly prefer that the processors and willing banks step forward and simply shoulder the responsibility and then compete with each other on price and end-customer convenience.

---

[15] "The Five Layers of Fraud Prevention and Using Them to Beat Malware". Gartner. http://my.gartner.com/portal/server.pt?open=512&objID=249&mode=2&PageID=864059&resId=1646115&ref=Browse

Another non-legislative step in the right direction is to find a way to remind all government officials at the local, state, and federal levels, who make decisions on where taxpayer monies will be deposited, that they have a duty not to allow said funds to be stolen. This means no taxpayer funds could be directly or indirectly (e.g., an advance payment to a private contractor) being deposited at any F.I. where "shared responsibility" is their policy.

I believe we could get almost all existing victims made whole if public fiduciaries took the position that if any customer of a given bank has ever lost a dime to account takeover, even if they have signed a settlement agreement over the matter, no taxpayer money may be put at risk there, regardless of what new policy/security measures had been put in place since. In theory, it's possible that the losses from account takeover might be too large for a small bank to bear, but if this has ever truly happened, it has just been once. If necessary, restitution could be limited to some fraction of the bank's reserves.

The Federal Reserve has in the past imposed policies I don't agree with on America's financial services institutions by making it known that it would not approve a merger or acquisition where a bank not complying was on either side of the transaction was not in compliance. If there were any acceptable Fed power, getting banks to drop "shared responsibility" and adopt the stronger security measures their processors have been trying to sell them for years would be one.

But really, I have said my piece. The part of the ABA's position that I cannot support is its insistence that it is the prerogative of its member banks' executives to decide which victims get reimbursed what percentage of their losses, or at most it is a matter for the courts. In a contract dispute, the winner typically cannot recover legal costs from the loser, so for most victims a lawsuit would cost more than they would recover. The victims of account takeover cannot see how the decision about what to do about a new and fast-growing crime that picks off randomly unlucky American churches, school districts, public libraries, medical practices, charities, and small businesses can be made by anyone but the elected representatives of the people.

On the other hand, I am confident in my statement that, at the end of the day, the only way to stop account takeover rather than just continue to talk about it (and also litigate about it), is to concentrate the actual operation of online banking systems in the hands of a smaller number of organizations that answer to the description of the processors I give above. The very largest banks, most especially the ones that provide adequate security, are their own online banking processors. But even if the Congress enables the FFIEC to issue its Guidance to the 13 processors as well as banks that run their own online banking, at least we will be subtracting more regulation than we are adding. The 14 pages of the FFIEC 2005 Guidance, plus the 8 pages of the 2011 Guidance plus Gartner's 10 pages about the five layers of fraud controls and the security products that fit within them would have to be read and understood by only 13 big companies rather than their 5,000+ small- and medium-sized bank customers.

The bad news is that if you do nothing, I can assure you the problem will only get much worse and very soon.

The good news is that among all the complex, difficult, deeply partisan and often controversial problems that lay at your feet everyday; this one—this problem, though very serious and very dangerous is also:

1. Very non-partisan and
2. Very fixable by bright and dedicated people like yourselves.

My only request is that you fix it now, before more money flows to our enemies and becomes too big to fix.

Thank you very much for, first, holding this important hearing. And secondly, thank you for allowing me to participate.

James R. Woodhill
Advocate, Government and Public Relations
YourMoneyIsNotSafeInTheBank.org

Relevant recent testimonies:

FBI Assistant Director Gordon Snow Testimony –

http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

In his September 14, 2011 testimony before the Subcommittee on Financial Institutions and Consumer Credit, Assistant FBI Director Gordon M. Snow presented the authoritative account of ACH fraud, among many others.

Entrust CEO/President Bill Conner Testimony –

http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=9250

The testimony of Bill Conner, President and CEO of Entrust, before the Subcommittee on Communications and Technology of the House Committee on Energy, entitled "Cybersecurity: Threats to Communications Networks and Private-‐Sector Responses", on February 8, 2012, offers details of this crime and how it is intertwined with the general problem of reliably establishing the identities of actors in cyberspace.

Questions Submitted by Representative Schweikert
Hearing: "Cyber Threats to Capital Markets and Corporate Accounts"
June 1, 2012

1. The FS-ISAC partnership with Microsoft on the "botnet" takedown sounds very interesting. What more can you tell us about it?
2. Taking down a botnet's command-and-control server still leaves the malware in place on individual computers if another crook could manage to regain control. Should the government have a policy on how to actually eliminate the botnet software and not just temporarily behead the botnet itself? Is there any planning for dealing with botnets on anything other than an ad hoc basis?

DRAFT Answer for Question #1:

Botnet Takedown Partnership with Microsoft

FS-ISAC, in partnership with Microsoft and NACHA, announced on March 26, 2012, that they successfully executed a coordinated global takedown operation against some of the most notorious cybercrime operations responsible for online fraud and identity theft. The takedown was accomplished through coordinated legal and technical actions and disrupted massive botnets using the ZeuS and SpyEye malware families, striking a major blow against cybercriminal operators targeting the financial services sector's customers.

A video news release about the disruption, codenamed, "Operation B71", is located here at the Microsoft Digital Crimes Unit web page: http://www.microsoft.com/presspass/presskits/dcu/

The takedown will help prevent online fraud and identity theft for consumers and businesses worldwide. Microsoft's investigation shows that approximately 3.6 million computers in the United States alone have been infected with the ZeuS malware.

This takedown was made possible through a successful pleading before the U.S. District Court for the Eastern District of New York on March 19, 2012, which allowed Microsoft, FS-ISAC and NACHA to sever the command and control structures of several of the most dangerous botnets running ZeuS, SpyEye and Ice IX malware. Because the botnet operators used ZeuS, SpyEye and Ice IX to steal victims' online banking credentials and transfer stolen funds, FS-ISAC and NACHA joined Microsoft as plaintiffs in the civil suit.

On March 23, 2012, Microsoft and co-plaintiffs FS-ISAC and NACHA, escorted by the U.S. Marshals Service, executed a coordinated physical seizure of servers in multiple hosting locations to preserve evidence for this case and seized hundreds of domain names used by the ZeuS, SpyEye and Ice IX malware to remotely command and control victim computers.

Although it is not expected that this operation will completely destroy all botnets running ZeuS, SpyEye and Ice IX malware, or even that every botnet taken down in the operation will stay down permanently, this action is expected to significantly disrupt the cybercriminals' operations by increasing the risk and costs for its controllers to continue doing business.

Microsoft will use the intelligence gained from this takedown to partner with Internet Service Providers and Computer Emergency Response Teams around the world to help remediate infected computers from the control of ZeuS, SpyEye and Ice IX. It is likely that the infected computers are infected with other malware as well. The remediation plans would include eradication of all other known malware, making the Internet safer for consumers and businesses worldwide.

Together, these aspects of the operation are expected to undermine the criminal infrastructure that relies on these botnets every day to make money and helps to provide new tools for the industry to work together to proactively fight cybercrime.

DRAFT Answer for Question #2:
Industry, partnering with government, has many efforts already underway that are proactive, voluntary and coordinated. It is important to highlight that no one company, organization, government or system by itself has the ability to reduce the risk posed from botnets. Working together in a coordinated and strategic way we can make an impact. The FS-ISAC is proud to be a part of these types of efforts.

Working together with our partners in industry and government we have taken and will continue to take positive and affirmative steps toward reducing the risk to our customers posed by botnets and malware. As discussed above, the financial services sector is working closely with Microsoft to undertake defensive legal actions, but this is only one piece of the overall effort to reduce the systemic risk posed by botnets. Controlling the botnet problem requires a holistic and repeatable approach that is grounded in open lines of communication, the ability to coordinate actions and the policy in place to support it. It takes a great deal of planning, prepositioning of operational relationships and information sharing to understand the threat, develop the appropriate mitigation plan and then implement it - often times across borders and jurisdictions.

Over the past year, the FS-ISAC has been involved in a number of key initiatives that seek to improve policies, procedures, information sharing and ultimately defensive operations across a number of sectors. Key examples include:

1. In March 2012, an industry advisory group for the Federal Communications Commission (FCC), the Communications, Security, Reliability, and Interoperability Council (CSRIC), unanimously adopted recommendations for voluntary action by Internet service providers (ISPs) to combat three major cybersecurity threats, including botnets, such as those targeted in the Operation B71. CSRIC has endorsed industry-based recommendations for an Anti-Bot Code of Conduct where the ISPs agree to educate consumers about the botnet threat, take steps to detect botnet activity on their networks, make consumers aware of botnet infections on their computers, offer assistance to consumers whose computers are infected and collaborate with other service providers that have also adopted the Anti-Bot Code.

2. Stemming from the relationship and policy work above, the FS-ISAC is coordinating a cross-sector Botnet Mitigation working group. The working group is currently investigating ways for financial institutions to share suspected and known botnet infection of their customers with participating mitigation partners, including many of the

largest Internet Service Providers in the country. The working group will create a process whereby financial institutions can share botnet information quickly with mitigation partners. The mitigation partners would in turn work to notify and, where possible and appropriate, help to remediate the impacted customer systems. We believe this approach provides a more comprehensive, long term, scalable and repeatable capability to address the malware / botnet problem.

3. FS-ISAC is also a part of the Industry Botnet Group (IBG) which is a voluntary group of companies, trade associations, and non-profit organizations concerned about defending the Internet ecosystem from the proliferation of botnets and other malicious activity online. The IBG was established in January 2012 to collaborate, share expertise and aggregate resources to combat botnets. The IBG is comprised of members who voluntarily participate and are focused on the following areas:
    - Raising awareness of the threat of botnets;
    - Encouraging prevention;
    - Improving detection;
    - Notifying computer users who are infected;
    - Providing access to remediation resources; and
    - Ensuring a speedy recovery from the impact of botnets and malware.

Whether it be through the involvement in a full botnet takedown operation or through the disruption of a botnet's infrastructure, the FS-ISAC aims to cooperate with industry, law enforcement, academia, government, and other non-Governmental Organizations worldwide to put cybercriminals out of business and help the global Internet community protect itself and thrive.